



WSNOC-25.12.0.7177260526-FP1-S

Delivery Notes

Author	Prashanth Pillai
Owner	Subbe Subbegowda
Approver	Subbe Subbegowda
Organization	Optical Networks Automation
Document type	Delivery Notes
Document version	1.0
Document location	ALED-OLCS

Contents

1	About this Document.....	3
2	Software Composition.....	4
	2.1 Patch Location.....	4
	2.2 MD5, Checksum and Size Values.....	4
3	Contents	5
	3.1 Fixed Tickets.....	5
4	Installation.....	6

1 About this Document

Scope

The scope of the document is to provide the release notes for WSNOC-25.12.0.7177260526-FP1-S

2 Software Composition

2.1 Patch Location

WSNOC-25.12.0.7177260526-FP1-S is available on OLCS.

2.2 MD5, Checksum and Size Values

Package	Checksum	Size	Md5sum
mnc-plat-25.12.0-7177260526-FP1SMay2026.iso (3PP: 25.12.0:81)	2282392983	8518995968	948d010c269653d450d34f3568d8e51b
mnc-oracle-25.12.0-7177260526-FP1SMay2026.iso	1143296890	2377811968	827c706fc47ec2f2eb01db0ffee91a34
wsnoc-sw-25.12.0-7177260526-FP1SMay2026.iso	2773863711	16099741696	a1fc6eac60250a2472506bd18d6d8ffa
ws-os-25.12.0-11.iso	2029759374	665602048	71ddb8d52e38d7dd3949d3ad01882c63

3 Contents

3.1 Fixed Vulnerabilities on WS-OS ISO

Package Name	Version	CVEs Addressed / Primary Fixes
kernel-modules-extra (and entire kernel z-stream)	4.18.0-553.124.1.el8_10	RHSA-2026:16195 → CVE-2026-43284 ("Dirty Frag" — universal Local Privilege Escalation via ESP XFRM in the kernel). Because build 10 shipped the GA 4.18.0-553.el8_10, this jump also pulls in ~20 intermediate z-stream advisories — e.g. RHSA-2026:13577 → CVE-2024-41073, CVE-2025-40252, CVE-2025-68724, CVE-2026-23401, CVE-2026-31402, CVE-2026-31431, CVE-2026-43077 — plus a long tail of cumulative backports across the scheduler, memory management, networking (TCP/IPv6/SMB/CIFS), and device drivers.
python3.12 / python3.12-libs	3.12.13-2.el8_10	RHSA-2026:10950 → CVE-2026-1502 (HTTP header injection), CVE-2026-4786 (command injection via crafted URL prefixes), CVE-2026-6100 (use-after-free in decompression modules), CVE-2025-59375 (bundled libexpat large-allocation DoS). Build 10 shipped 3.12.8, so this also rolls in RHSA-2026:6283 → CVE-2026-4519 (command-line option injection in webbrowser.open()) and the earlier 3.12.x z-stream fixes.
vim-common / vim-enhanced / vim-filesystem	8.0.1763-22.el8_10.3	RHSA-2026:11509 → CVE-2026-34982 (arbitrary command execution via modeline sandbox bypass — complete, guitabtooltip, printhead missing P_MLE; mapset() lacks check_secure()). Since build 10 was at -19.el8_6.4, this jump also rolls in RHSA-2026:4442 → CVE-2026-25749 (arbitrary code execution via helpfile option) and RHSA-2026:6915 → CVE-2026-28417 (OS command injection in netrw), CVE-2026-28421 (DoS / info disclosure via crafted swap file), CVE-2026-33412 (command injection in glob()).
jq	1.6-12.el8_10	RHSA-2026:16252 → CVE-2026-39979 (out-of-bounds read in jv_parse_sized() on non-NUL-terminated buffers), CVE-2026-40164 (DoS via crafted JSON object causing hash collisions in the hardcoded MurmurHash3 seed).
wget (Rocky only)	1.19.5-12.el8_10	RHSA-2024:5299 → CVE-2024-38428 (interpretation conflict — semicolons in URI userinfo subcomponent misinterpreted as part of host, enabling SSRF-style host substitution).
python3-setuptools / platform-	39.2.0-9.el8_10	RHSA-2025:11036 → CVE-2025-47273 (path traversal in PackageIndex). Because build 10 was at -7.el8, this jump also pulls in RHSA-2024:5530 → CVE-2024-6345 (remote code execution via download functions in package_index).

python-setuptools		Note: platform-python-setuptools is newly added in build 11 as part of the same RHSA.
container-selinux (container-tools:rhel8 module)	2.229.0-2.module+el8.10.0+24081+a04d358a	RHSA-2026:4672 → CVE-2025-61726 (Go net/url memory exhaustion in query parsing), CVE-2025-61728 (Go archive/zip excessive CPU when building archive index), CVE-2025-68121 (unexpected session resumption in Go crypto/tls). Module rebuild against the patched Go runtime.
chrony	4.5-2.el8_10	RHBA-2024:8855 — enables AES-CMAC support; fixes chronyd crash during reload. No CVEs.
dnsmasq	2.79-35.el8_10	RHBA-2025:17424 — fixes caching and query-forwarding regressions (RHEL-61943, RHEL-6586). No CVEs.
rng-tools	6.16-2.el8_10	Bug-fix rebuild for jitter-entropy stability. No CVEs.
tar (Rocky only)	1.30-11.el8_10	RHBA-2025:14556 — restores tar x --no-overwrite-dir behavior (regression from 1.30-9). No CVEs.
polycore utils / python3-polycore utils (Rocky)	2.9-26.el8_10	RHBA-2024:4253 — fixes semanage fcontext listing order and semanage export --modify/--add distinction. No CVEs.
libsemanage / python3-libsemanage (Rocky)	2.9-12.el8_10	RHBA-2025:8407 — fixes 10x slowdown in labelling (RHEL-86057). No CVEs.
audit / python3-audit (Rocky)	3.1.2-1.el8_10.1	RHBA-2025:11033 — fixes augenrules exit code in immutable mode and a rule-load break on /usr/lib/modules. No CVEs.

3.1.1 Fixed Vulnerabilities on red-hat OS (containers only)

CVE	Fixed By RPM(s)
CVE-2005-3625	cups-libs-2.2.6-67.el8_10.x86_64.rpm
CVE-2005-3626	cups-libs-2.2.6-67.el8_10.x86_64.rpm
CVE-2005-3627	cups-libs-2.2.6-67.el8_10.x86_64.rpm
CVE-2006-10002	perl-XML-Parser-2.44-12.el8_10.x86_64.rpm
CVE-2006-10003	perl-XML-Parser-2.44-12.el8_10.x86_64.rpm
CVE-2007-2445	libpng-1.6.34-10.el8_10.x86_64.rpm
CVE-2007-4045	cups-libs-2.2.6-67.el8_10.x86_64.rpm
CVE-2007-4352	cups-libs-2.2.6-67.el8_10.x86_64.rpm

CVE-2007-5269	libpng-1.6.34-10.el8_10.x86_64.rpm
CVE-2007-5392	cups-libs-2.2.6-67.el8_10.x86_64.rpm
CVE-2007-5393	cups-libs-2.2.6-67.el8_10.x86_64.rpm
CVE-2008-0047	cups-libs-2.2.6-67.el8_10.x86_64.rpm
CVE-2008-1373	cups-libs-2.2.6-67.el8_10.x86_64.rpm
CVE-2008-1382	libpng-1.6.34-10.el8_10.x86_64.rpm
CVE-2008-1722	cups-libs-2.2.6-67.el8_10.x86_64.rpm
CVE-2008-3639	cups-libs-2.2.6-67.el8_10.x86_64.rpm
CVE-2008-3640	cups-libs-2.2.6-67.el8_10.x86_64.rpm
CVE-2008-3641	cups-libs-2.2.6-67.el8_10.x86_64.rpm
CVE-2008-3964	libpng-1.6.34-10.el8_10.x86_64.rpm
CVE-2008-5183	cups-libs-2.2.6-67.el8_10.x86_64.rpm
CVE-2009-0040	libpng-1.6.34-10.el8_10.x86_64.rpm
CVE-2009-0163	cups-libs-2.2.6-67.el8_10.x86_64.rpm
CVE-2009-0164	cups-libs-2.2.6-67.el8_10.x86_64.rpm
CVE-2009-2042	libpng-1.6.34-10.el8_10.x86_64.rpm
CVE-2009-3553	cups-libs-2.2.6-67.el8_10.x86_64.rpm
CVE-2010-0205	libpng-1.6.34-10.el8_10.x86_64.rpm
CVE-2010-0302	cups-libs-2.2.6-67.el8_10.x86_64.rpm
CVE-2010-0540	cups-libs-2.2.6-67.el8_10.x86_64.rpm
CVE-2010-0542	cups-libs-2.2.6-67.el8_10.x86_64.rpm
CVE-2010-1205	libpng-1.6.34-10.el8_10.x86_64.rpm
CVE-2010-1748	cups-libs-2.2.6-67.el8_10.x86_64.rpm
CVE-2010-2249	libpng-1.6.34-10.el8_10.x86_64.rpm
CVE-2010-2526	device-mapper-1.02.181-15.el8_10.3.x86_64.rpm, device-mapper-libs-1.02.181-15.el8_10.3.x86_64.rpm
CVE-2010-2941	cups-libs-2.2.6-67.el8_10.x86_64.rpm
CVE-2011-2501	libpng-1.6.34-10.el8_10.x86_64.rpm
CVE-2011-2690	libpng-1.6.34-10.el8_10.x86_64.rpm
CVE-2011-2691	libpng-1.6.34-10.el8_10.x86_64.rpm
CVE-2011-2692	libpng-1.6.34-10.el8_10.x86_64.rpm
CVE-2011-2896	cups-libs-2.2.6-67.el8_10.x86_64.rpm
CVE-2011-3026	libpng-1.6.34-10.el8_10.x86_64.rpm
CVE-2011-3045	libpng-1.6.34-10.el8_10.x86_64.rpm
CVE-2011-3048	libpng-1.6.34-10.el8_10.x86_64.rpm
CVE-2011-3464	libpng-1.6.34-10.el8_10.x86_64.rpm
CVE-2012-5519	cups-libs-2.2.6-67.el8_10.x86_64.rpm
CVE-2014-3537	cups-libs-2.2.6-67.el8_10.x86_64.rpm
CVE-2014-5029	cups-libs-2.2.6-67.el8_10.x86_64.rpm
CVE-2014-5030	cups-libs-2.2.6-67.el8_10.x86_64.rpm
CVE-2014-5031	cups-libs-2.2.6-67.el8_10.x86_64.rpm
CVE-2015-8126	libpng-1.6.34-10.el8_10.x86_64.rpm

CVE-2017-12652	libpng-1.6.34-10.el8_10.x86_64.rpm
CVE-2017-18248	cups-libs-2.2.6-67.el8_10.x86_64.rpm
CVE-2018-12126	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2018-12127	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2018-12130	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2018-12207	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2018-13785	libpng-1.6.34-10.el8_10.x86_64.rpm
CVE-2018-14625	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2018-14633	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2018-15572	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2018-16658	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2018-16880	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2018-16884	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2018-17182	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2018-18021	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2018-18281	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2018-18397	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2018-18955	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2018-19407	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2018-19854	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2018-19985	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2018-20169	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2018-20669	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2018-20784	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2018-3620	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2018-3639	java-1.8.0-openjdk-1.8.0.492.b09-1.el8.x86_64.rpm, java-1.8.0-openjdk-devel-1.8.0.492.b09-1.el8.x86_64.rpm, java-1.8.0-openjdk-headless-1.8.0.492.b09-1.el8.x86_64.rpm
CVE-2018-3646	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2018-4180	cups-libs-2.2.6-67.el8_10.x86_64.rpm
CVE-2018-4181	cups-libs-2.2.6-67.el8_10.x86_64.rpm
CVE-2018-4182	cups-libs-2.2.6-67.el8_10.x86_64.rpm
CVE-2018-4183	cups-libs-2.2.6-67.el8_10.x86_64.rpm
CVE-2018-4700	cups-libs-2.2.6-67.el8_10.x86_64.rpm
CVE-2018-5391	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2018-9363	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2019-0154	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2019-0155	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2019-10126	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2019-10207	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2019-10639	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2019-11085	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm

CVE-2019-11091	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2019-11135	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2019-1125	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2019-11477	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2019-11478	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2019-11479	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2019-11487	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2019-11810	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2019-11833	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2019-11884	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2019-12614	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2019-12735	vim-common-8.0.1763-22.el8_10.x86_64.rpm, vim-enhanced-8.0.1763-22.el8_10.x86_64.rpm, vim-filestsystem-8.0.1763-22.el8_10.noarch.rpm, vim-minimal-8.0.1763-22.el8_10.x86_64.rpm
CVE-2019-13233	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2019-13272	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2019-13631	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2019-14821	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2019-14835	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2019-14895	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2019-14901	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2019-15099	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2019-1547	openssl-1.1.1k-15.el8_6.x86_64.rpm, openssl-devel-1.1.1k-15.el8_6.x86_64.rpm, openssl-libs-1.1.1k-15.el8_6.i686.rpm, openssl-libs-1.1.1k-15.el8_6.x86_64.rpm
CVE-2019-1549	openssl-1.1.1k-15.el8_6.x86_64.rpm, openssl-devel-1.1.1k-15.el8_6.x86_64.rpm, openssl-libs-1.1.1k-15.el8_6.i686.rpm, openssl-libs-1.1.1k-15.el8_6.x86_64.rpm
CVE-2019-15505	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2019-1563	openssl-1.1.1k-15.el8_6.x86_64.rpm, openssl-devel-1.1.1k-15.el8_6.x86_64.rpm, openssl-libs-1.1.1k-15.el8_6.i686.rpm, openssl-libs-1.1.1k-15.el8_6.x86_64.rpm
CVE-2019-15847	cpp-8.5.0-28.el8_10.x86_64.rpm, gcc-8.5.0-28.el8_10.x86_64.rpm, gcc-c++-8.5.0-28.el8_10.x86_64.rpm, gcc-plugin-annobin-8.5.0-28.el8_10.x86_64.rpm, libgcc-8.5.0-28.el8_10.i686.rpm, libgcc-8.5.0-28.el8_10.x86_64.rpm, libgomp-8.5.0-28.el8_10.x86_64.rpm, libstdc++-8.5.0-28.el8_10.i686.rpm, libstdc++-8.5.0-28.el8_10.x86_64.rpm, libstdc++-devel-8.5.0-28.el8_10.x86_64.rpm
CVE-2019-15925	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2019-16231	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2019-16233	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2019-17053	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm

CVE-2019-17055	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2019-17133	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2019-17666	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2019-18808	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2019-18809	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2019-19056	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2019-19057	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2019-19062	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2019-19063	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2019-19068	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2019-19072	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2019-19073	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2019-19074	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2019-19319	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2019-19332	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2019-19338	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2019-19524	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2019-19533	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2019-19534	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2019-19543	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2019-19767	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2019-19770	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2019-20054	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2019-20636	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2019-20807	vim-common-8.0.1763-22.el8_10.x86_64.rpm, vim-enhanced-8.0.1763-22.el8_10.x86_64.rpm, vim-filesystem-8.0.1763-22.el8_10.noarch.rpm, vim-minimal-8.0.1763-22.el8_10.x86_64.rpm
CVE-2019-25162	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2019-3459	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2019-3819	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2019-3846	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2019-3874	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2019-3882	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2019-3887	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2019-3892	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2019-5489	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2019-6974	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2019-7221	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2019-7222	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2019-7308	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2019-8675	cups-libs-2.2.6-67.el8_10.x86_64.rpm

CVE-2019-8696	cups-libs-2.2.6-67.el8_10.x86_64.rpm
CVE-2019-8912	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2019-8956	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2019-8980	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2019-9213	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2019-9455	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2019-9458	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2019-9500	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2019-9506	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2020-0305	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2020-0404	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2020-0427	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2020-0466	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2020-0543	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2020-10001	cups-libs-2.2.6-67.el8_10.x86_64.rpm
CVE-2020-10711	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2020-10713	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2020-10732	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2020-10751	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2020-10757	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2020-10766	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2020-10767	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2020-10768	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2020-10773	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2020-10774	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2020-10942	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2020-11023	cpp-8.5.0-28.el8_10.x86_64.rpm, gcc-8.5.0-28.el8_10.x86_64.rpm, gcc-c++-8.5.0-28.el8_10.x86_64.rpm, gcc-plugin-annobin-8.5.0-28.el8_10.x86_64.rpm, libgcc-8.5.0-28.el8_10.i686.rpm, libgcc-8.5.0-28.el8_10.x86_64.rpm, libgomp-8.5.0-28.el8_10.x86_64.rpm, libstdc++-8.5.0-28.el8_10.i686.rpm, libstdc++-8.5.0-28.el8_10.x86_64.rpm, libstdc++-devel-8.5.0-28.el8_10.x86_64.rpm
CVE-2020-11565	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2020-11884	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2020-12114	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2020-12351	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2020-12352	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2020-12362	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2020-12655	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2020-12826	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2020-12888	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2020-13974	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm

CVE-2020-14314	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2020-14331	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2020-14351	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2020-14356	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2020-14385	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2020-14386	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2020-15437	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2020-16166	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2020-1971	openssl-1.1.1k-15.el8_6.x86_64.rpm, openssl-devel-1.1.1k-15.el8_6.x86_64.rpm, openssl-libs-1.1.1k-15.el8_6.i686.rpm, openssl-libs-1.1.1k-15.el8_6.x86_64.rpm
CVE-2020-24490	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2020-24502	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2020-24503	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2020-24504	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2020-24586	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2020-24587	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2020-24588	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2020-25211	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2020-25212	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2020-25284	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2020-25285	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2020-25643	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2020-25645	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2020-25656	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2020-25659	openssl-1.1.1k-15.el8_6.x86_64.rpm, openssl-devel-1.1.1k-15.el8_6.x86_64.rpm, openssl-libs-1.1.1k-15.el8_6.i686.rpm, openssl-libs-1.1.1k-15.el8_6.x86_64.rpm
CVE-2020-26139	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2020-26141	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2020-26144	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2020-26145	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2020-26147	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2020-26541	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2020-26555	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2020-2732	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2020-27777	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2020-27820	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2020-27835	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2020-28374	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2020-28974	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2020-29368	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm

CVE-2020-29660	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2020-29661	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2020-35508	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2020-36158	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2020-36516	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2020-36777	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2020-3898	cups-libs-2.2.6-67.el8_10.x86_64.rpm
CVE-2020-8252	libuv-1.41.1-2.el8_10.x86_64.rpm
CVE-2020-8647	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2020-8648	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2020-8649	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2021-0342	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2021-0920	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2021-20239	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2021-20321	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2021-20322	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2021-21781	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2021-26341	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2021-26401	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2021-26708	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2021-27363	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2021-27364	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2021-27365	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2021-29155	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2021-30002	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2021-31829	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2021-33034	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2021-33200	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2021-33631	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2021-33655	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2021-33656	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2021-3449	openssl-1.1.1k-15.el8_6.x86_64.rpm, openssl-devel-1.1.1k-15.el8_6.x86_64.rpm, openssl-libs-1.1.1k-15.el8_6.i686.rpm, openssl-libs-1.1.1k-15.el8_6.x86_64.rpm
CVE-2021-3450	openssl-1.1.1k-15.el8_6.x86_64.rpm, openssl-devel-1.1.1k-15.el8_6.x86_64.rpm, openssl-libs-1.1.1k-15.el8_6.i686.rpm, openssl-libs-1.1.1k-15.el8_6.x86_64.rpm
CVE-2021-3501	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2021-3542	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2021-3564	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2021-3573	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2021-3609	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm

CVE-2021-3653	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2021-3656	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2021-3659	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2021-3669	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2021-3679	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2021-3712	openssl-1.1.1k-15.el8_6.x86_64.rpm, openssl-devel-1.1.1k-15.el8_6.x86_64.rpm, openssl-libs-1.1.1k-15.el8_6.i686.rpm, openssl-libs-1.1.1k-15.el8_6.x86_64.rpm
CVE-2021-37159	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2021-3732	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2021-3753	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2021-37576	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2021-3759	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2021-3773	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2021-3778	vim-common-8.0.1763-22.el8_10.x86_64.rpm, vim-enhanced-8.0.1763-22.el8_10.x86_64.rpm, vim-filesystem-8.0.1763-22.el8_10.noarch.rpm, vim-minimal-8.0.1763-22.el8_10.x86_64.rpm
CVE-2021-3796	vim-common-8.0.1763-22.el8_10.x86_64.rpm, vim-enhanced-8.0.1763-22.el8_10.x86_64.rpm, vim-filesystem-8.0.1763-22.el8_10.noarch.rpm, vim-minimal-8.0.1763-22.el8_10.x86_64.rpm
CVE-2021-3872	vim-common-8.0.1763-22.el8_10.x86_64.rpm, vim-enhanced-8.0.1763-22.el8_10.x86_64.rpm, vim-filesystem-8.0.1763-22.el8_10.noarch.rpm, vim-minimal-8.0.1763-22.el8_10.x86_64.rpm
CVE-2021-3984	vim-common-8.0.1763-22.el8_10.x86_64.rpm, vim-enhanced-8.0.1763-22.el8_10.x86_64.rpm, vim-filesystem-8.0.1763-22.el8_10.noarch.rpm, vim-minimal-8.0.1763-22.el8_10.x86_64.rpm
CVE-2021-4002	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2021-4019	vim-common-8.0.1763-22.el8_10.x86_64.rpm, vim-enhanced-8.0.1763-22.el8_10.x86_64.rpm, vim-filesystem-8.0.1763-22.el8_10.noarch.rpm, vim-minimal-8.0.1763-22.el8_10.x86_64.rpm
CVE-2021-4028	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2021-4083	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2021-4155	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2021-41864	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2021-4192	vim-common-8.0.1763-22.el8_10.x86_64.rpm, vim-enhanced-8.0.1763-22.el8_10.x86_64.rpm, vim-filesystem-8.0.1763-22.el8_10.noarch.rpm, vim-minimal-8.0.1763-22.el8_10.x86_64.rpm

CVE-2021-4193	vim-common-8.0.1763-22.el8_10.x86_64.rpm, vim-enhanced-8.0.1763-22.el8_10.x86_64.rpm, vim-filessystem-8.0.1763-22.el8_10.noarch.rpm, vim-minimal-8.0.1763-22.el8_10.x86_64.rpm
CVE-2021-4203	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2021-4204	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2021-43056	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2021-43267	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2021-43389	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2021-44733	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2021-45485	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2021-45486	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2021-46909	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2021-46934	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2021-46939	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2021-46972	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2021-46984	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2021-47013	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2021-47018	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2021-47055	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2021-47069	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2021-47073	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2021-47097	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2021-47101	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2021-47118	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2021-47153	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2021-47171	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2021-47185	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2021-47236	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2021-47257	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2021-47284	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2021-47287	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2021-47289	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2021-47304	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2021-47310	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2021-47311	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2021-47321	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2021-47338	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2021-47352	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2021-47353	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2021-47356	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2021-47373	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm

CVE-2021-47383	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2021-47384	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2021-47385	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2021-47386	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2021-47393	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2021-47408	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2021-47412	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2021-47432	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2021-47441	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2021-47455	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2021-47456	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2021-47461	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2021-47466	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2021-47468	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2021-47491	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2021-47495	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2021-47497	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2021-47527	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2021-47548	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2021-47560	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2021-47579	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2021-47582	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2021-47609	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2021-47624	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2021-47670	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-0001	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-0002	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-0185	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-0261	vim-common-8.0.1763-22.el8_10.x86_64.rpm, vim-enhanced-8.0.1763-22.el8_10.x86_64.rpm, vim-filesystem-8.0.1763-22.el8_10.noarch.rpm, vim-minimal-8.0.1763-22.el8_10.x86_64.rpm
CVE-2022-0318	vim-common-8.0.1763-22.el8_10.x86_64.rpm, vim-enhanced-8.0.1763-22.el8_10.x86_64.rpm, vim-filesystem-8.0.1763-22.el8_10.noarch.rpm, vim-minimal-8.0.1763-22.el8_10.x86_64.rpm
CVE-2022-0330	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-0359	vim-common-8.0.1763-22.el8_10.x86_64.rpm, vim-enhanced-8.0.1763-22.el8_10.x86_64.rpm, vim-filesystem-8.0.1763-22.el8_10.noarch.rpm, vim-minimal-8.0.1763-22.el8_10.x86_64.rpm
CVE-2022-0361	vim-common-8.0.1763-22.el8_10.x86_64.rpm, vim-enhanced-8.0.1763-22.el8_10.x86_64.rpm, vim-filesystem-8.0.1763-

	22.el8_10.noarch.rpm, vim-minimal-8.0.1763-22.el8_10.x86_64.rpm
CVE-2022-0392	vim-common-8.0.1763-22.el8_10.x86_64.rpm, vim-enhanced-8.0.1763-22.el8_10.x86_64.rpm, vim-filesystem-8.0.1763-22.el8_10.noarch.rpm, vim-minimal-8.0.1763-22.el8_10.x86_64.rpm
CVE-2022-0413	vim-common-8.0.1763-22.el8_10.x86_64.rpm, vim-enhanced-8.0.1763-22.el8_10.x86_64.rpm, vim-filesystem-8.0.1763-22.el8_10.noarch.rpm, vim-minimal-8.0.1763-22.el8_10.x86_64.rpm
CVE-2022-0435	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-0492	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-0494	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-0500	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-0516	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-0617	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-0778	openssl-1.1.1k-15.el8_6.x86_64.rpm, openssl-devel-1.1.1k-15.el8_6.x86_64.rpm, openssl-libs-1.1.1k-15.el8_6.i686.rpm, openssl-libs-1.1.1k-15.el8_6.x86_64.rpm
CVE-2022-0847	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-0854	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-1011	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-1012	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-1015	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-1016	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-1154	vim-common-8.0.1763-22.el8_10.x86_64.rpm, vim-enhanced-8.0.1763-22.el8_10.x86_64.rpm, vim-filesystem-8.0.1763-22.el8_10.noarch.rpm, vim-minimal-8.0.1763-22.el8_10.x86_64.rpm
CVE-2022-1184	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-1292	openssl-1.1.1k-15.el8_6.x86_64.rpm, openssl-devel-1.1.1k-15.el8_6.x86_64.rpm, openssl-libs-1.1.1k-15.el8_6.i686.rpm, openssl-libs-1.1.1k-15.el8_6.x86_64.rpm
CVE-2022-1462	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-1621	vim-common-8.0.1763-22.el8_10.x86_64.rpm, vim-enhanced-8.0.1763-22.el8_10.x86_64.rpm, vim-filesystem-8.0.1763-22.el8_10.noarch.rpm, vim-minimal-8.0.1763-22.el8_10.x86_64.rpm
CVE-2022-1629	vim-common-8.0.1763-22.el8_10.x86_64.rpm, vim-enhanced-8.0.1763-22.el8_10.x86_64.rpm, vim-filesystem-8.0.1763-22.el8_10.noarch.rpm, vim-minimal-8.0.1763-22.el8_10.x86_64.rpm
CVE-2022-1679	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm

CVE-2022-1785	vim-common-8.0.1763-22.el8_10.x86_64.rpm, vim-enhanced-8.0.1763-22.el8_10.x86_64.rpm, vim-filesystem-8.0.1763-22.el8_10.noarch.rpm, vim-minimal-8.0.1763-22.el8_10.x86_64.rpm
CVE-2022-1789	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-1897	vim-common-8.0.1763-22.el8_10.x86_64.rpm, vim-enhanced-8.0.1763-22.el8_10.x86_64.rpm, vim-filesystem-8.0.1763-22.el8_10.noarch.rpm, vim-minimal-8.0.1763-22.el8_10.x86_64.rpm
CVE-2022-1927	vim-common-8.0.1763-22.el8_10.x86_64.rpm, vim-enhanced-8.0.1763-22.el8_10.x86_64.rpm, vim-filesystem-8.0.1763-22.el8_10.noarch.rpm, vim-minimal-8.0.1763-22.el8_10.x86_64.rpm
CVE-2022-1966	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-20141	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-2068	openssl-1.1.1k-15.el8_6.x86_64.rpm, openssl-devel-1.1.1k-15.el8_6.x86_64.rpm, openssl-libs-1.1.1k-15.el8_6.i686.rpm, openssl-libs-1.1.1k-15.el8_6.x86_64.rpm
CVE-2022-2078	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-2097	openssl-1.1.1k-15.el8_6.x86_64.rpm, openssl-devel-1.1.1k-15.el8_6.x86_64.rpm, openssl-libs-1.1.1k-15.el8_6.i686.rpm, openssl-libs-1.1.1k-15.el8_6.x86_64.rpm
CVE-2022-21123	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-21125	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-21166	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-21499	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-2196	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-22942	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-23222	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-23816	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-23825	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-23960	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-25265	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-25636	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-2586	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-2588	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-26373	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-2663	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-26691	cups-libs-2.2.6-67.el8_10.x86_64.rpm
CVE-2022-27666	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-28388	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-28390	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-2873	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-2964	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm

CVE-2022-29900	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-29901	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-3028	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-30594	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-3239	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-3522	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-3545	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-3564	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-3565	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-3566	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-3567	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-3594	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-3619	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-3623	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-3628	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-3640	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-36946	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-38096	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-39188	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-39189	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-40982	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-41218	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-41222	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-4129	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-4139	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-41674	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-41858	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-4269	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-42703	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-42720	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-42721	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-42722	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-42895	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-42896	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-4304	openssl-1.1.1k-15.el8_6.x86_64.rpm, openssl-devel-1.1.1k-15.el8_6.x86_64.rpm, openssl-libs-1.1.1k-15.el8_6.i686.rpm, openssl-libs-1.1.1k-15.el8_6.x86_64.rpm
CVE-2022-43750	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-4378	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-43945	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm

CVE-2022-4450	openssl-1.1.1k-15.el8_6.x86_64.rpm, openssl-devel-1.1.1k-15.el8_6.x86_64.rpm, openssl-libs-1.1.1k-15.el8_6.i686.rpm, openssl-libs-1.1.1k-15.el8_6.x86_64.rpm
CVE-2022-45869	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-45884	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-45886	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-45887	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-45919	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-45934	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-4744	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-47929	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-48619	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-48627	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-48632	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-48669	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-48743	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-48747	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-48754	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-48757	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-48760	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-48773	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-48804	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-48836	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-48866	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-48919	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-48936	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-49011	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-49058	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-49111	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-49136	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-49395	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-49788	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-49846	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-49938	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-49977	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-49985	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-50020	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-50087	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-50228	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-50367	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-50386	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-50543	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm

CVE-2022-50673	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2022-50865	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-0215	openssl-1.1.1k-15.el8_6.x86_64.rpm, openssl-devel-1.1.1k-15.el8_6.x86_64.rpm, openssl-libs-1.1.1k-15.el8_6.i686.rpm, openssl-libs-1.1.1k-15.el8_6.x86_64.rpm
CVE-2023-0266	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-0286	openssl-1.1.1k-15.el8_6.x86_64.rpm, openssl-devel-1.1.1k-15.el8_6.x86_64.rpm, openssl-libs-1.1.1k-15.el8_6.i686.rpm, openssl-libs-1.1.1k-15.el8_6.x86_64.rpm
CVE-2023-0386	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-0394	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-0458	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-0461	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-0597	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-1073	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-1075	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-1079	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-1118	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-1192	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-1206	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-1252	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-1281	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-1380	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-1382	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-1513	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-1637	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-1829	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-1838	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-1855	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-1989	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-1998	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-2002	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-20569	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-20588	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-20593	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-2124	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-2162	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-2163	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-2166	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-2194	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-2235	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-2248	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm

CVE-2023-23454	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-23455	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-24023	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-2483	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-2513	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-25775	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-26545	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-28464	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-28466	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-28772	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-30456	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-3090	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-31083	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-31084	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-3141	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-31436	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-3161	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-3212	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-32233	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-32324	cups-libs-2.2.6-67.el8_10.x86_64.rpm
CVE-2023-32360	cups-libs-2.2.6-67.el8_10.x86_64.rpm
CVE-2023-3268	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-3390	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-34241	cups-libs-2.2.6-67.el8_10.x86_64.rpm
CVE-2023-3446	openssl-1.1.1k-15.el8_6.x86_64.rpm, openssl-devel-1.1.1k-15.el8_6.x86_64.rpm, openssl-libs-1.1.1k-15.el8_6.i686.rpm, openssl-libs-1.1.1k-15.el8_6.x86_64.rpm
CVE-2023-35001	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-3567	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-35788	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-35823	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-35824	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-35825	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-3609	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-3611	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-37453	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-3772	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-3776	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-3812	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-3817	openssl-1.1.1k-15.el8_6.x86_64.rpm, openssl-devel-1.1.1k-15.el8_6.x86_64.rpm, openssl-libs-1.1.1k-15.el8_6.i686.rpm, openssl-libs-1.1.1k-15.el8_6.x86_64.rpm

CVE-2023-38409	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-39189	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-39192	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-39193	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-39194	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-39198	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-4004	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-40283	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-4128	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-4133	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-4155	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-4244	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-42752	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-42753	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-42754	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-42755	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-45863	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-45871	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-4622	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-46813	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-5090	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-51042	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-51779	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-5178	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-51780	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-52340	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-52434	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-52439	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-52445	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-52448	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-52451	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-52463	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-52464	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-52469	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-52470	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-52471	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-52476	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-52477	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-52478	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-52486	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-52489	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-52492	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm

CVE-2023-52513	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-52520	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-52522	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-52528	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-52530	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-52560	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-52565	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-52578	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-52594	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-52595	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-52598	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-52605	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-52606	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-52607	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-52610	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-52615	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-52619	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-52622	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-52623	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-52626	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-52648	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-52653	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-52658	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-52662	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-52667	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-52669	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-52675	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-52679	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-52683	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-52686	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-52700	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-52703	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-52707	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-52730	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-52752	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-52756	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-52762	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-52764	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-52775	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-52777	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-52781	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-52784	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm

CVE-2023-52791	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-52796	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-52798	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-52800	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-52803	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-52809	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-52811	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-52813	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-52817	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-52832	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-52834	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-52835	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-52840	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-52845	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-52847	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-52864	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-52877	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-52878	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-52922	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-52932	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-53052	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-53125	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-53178	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-53226	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-53246	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-53257	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-53297	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-53305	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-53373	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-53386	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-53401	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-53513	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-53539	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-53552	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-53673	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-53762	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-54076	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-54134	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-5633	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-5678	openssl-1.1.1k-15.el8_6.x86_64.rpm, openssl-devel-1.1.1k-15.el8_6.x86_64.rpm, openssl-libs-1.1.1k-15.el8_6.i686.rpm, openssl-libs-1.1.1k-15.el8_6.x86_64.rpm

CVE-2023-5717	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-6040	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-6121	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-6176	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-6240	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-6356	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-6535	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-6536	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-6546	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-6606	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-6610	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-6622	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-6817	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-6915	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-6931	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2023-6932	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-0340	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-0565	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-0646	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-0841	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-1086	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-12243	gnutls-3.6.16-8.el8_10.5.i686.rpm, gnutls-3.6.16-8.el8_10.5.x86_64.rpm, gnutls-dane-3.6.16-8.el8_10.5.x86_64.rpm, gnutls-utils-3.6.16-8.el8_10.5.x86_64.rpm
CVE-2024-21823	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-2201	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-23307	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-23848	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-24806	libuv-1.41.1-2.el8_10.x86_64.rpm
CVE-2024-24857	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-25739	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-25742	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-25743	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-25744	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-26583	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-26584	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-26585	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-26586	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-26593	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-26595	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-26600	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-26602	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm

CVE-2024-26603	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-26610	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-26614	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-26615	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-26638	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-26640	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-26642	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-26643	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-26645	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-26649	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-26656	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-26659	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-26660	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-26664	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-26665	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-26669	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-26675	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-26686	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-26693	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-26694	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-26704	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-26717	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-26720	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-26733	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-26735	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-26740	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-26743	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-26744	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-26759	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-26766	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-26769	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-26772	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-26773	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-26779	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-26782	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-26801	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-26802	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-26804	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-26810	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-26822	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-26826	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-26837	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm

CVE-2024-26840	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-26843	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-26846	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-26851	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-26852	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-26853	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-26855	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-26859	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-26870	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-26872	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-26878	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-26880	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-26892	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-26894	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-26897	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-26901	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-26906	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-26907	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-26908	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-26919	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-26921	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-26923	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-26924	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-26925	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-26929	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-26930	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-26931	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-26933	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-26934	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-26939	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-26940	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-26958	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-26960	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-26961	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-26964	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-26973	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-26974	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-26976	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-26982	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-26984	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-26993	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-27010	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm

CVE-2024-27011	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-27013	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-27014	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-27017	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-27019	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-27020	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-27025	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-27042	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-27043	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-27048	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-27052	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-27056	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-27059	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-27062	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-27065	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-27316	libnghttp2-1.33.0-6.el8_10.2.x86_64.rpm
CVE-2024-27388	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-27395	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-27397	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-27399	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-27410	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-27434	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-2961	glibc-2.28-251.el8_10.34.i686.rpm, glibc-2.28-251.el8_10.34.x86_64.rpm, glibc-common-2.28-251.el8_10.34.x86_64.rpm, glibc-devel-2.28-251.el8_10.34.x86_64.rpm, glibc-gconv-extra-2.28-251.el8_10.34.i686.rpm, glibc-gconv-extra-2.28-251.el8_10.34.x86_64.rpm, glibc-headers-2.28-251.el8_10.34.x86_64.rpm, glibc-langpack-en-2.28-251.el8_10.34.x86_64.rpm, glibc-minimal-langpack-2.28-251.el8_10.34.x86_64.rpm, libnsl-2.28-251.el8_10.34.i686.rpm, libnsl-2.28-251.el8_10.34.x86_64.rpm
CVE-2024-31076	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-33599	glibc-2.28-251.el8_10.34.i686.rpm, glibc-2.28-251.el8_10.34.x86_64.rpm, glibc-common-2.28-251.el8_10.34.x86_64.rpm, glibc-devel-2.28-251.el8_10.34.x86_64.rpm, glibc-gconv-extra-2.28-251.el8_10.34.i686.rpm, glibc-gconv-extra-2.28-251.el8_10.34.x86_64.rpm, glibc-headers-2.28-251.el8_10.34.x86_64.rpm, glibc-langpack-en-2.28-251.el8_10.34.x86_64.rpm, glibc-minimal-langpack-2.28-251.el8_10.34.x86_64.rpm, libnsl-2.28-251.el8_10.34.i686.rpm, libnsl-2.28-251.el8_10.34.x86_64.rpm

CVE-2024-33600	glibc-2.28-251.el8_10.34.i686.rpm, glibc-2.28-251.el8_10.34.x86_64.rpm, glibc-common-2.28-251.el8_10.34.x86_64.rpm, glibc-devel-2.28-251.el8_10.34.x86_64.rpm, glibc-gconv-extra-2.28-251.el8_10.34.i686.rpm, glibc-gconv-extra-2.28-251.el8_10.34.x86_64.rpm, glibc-headers-2.28-251.el8_10.34.x86_64.rpm, glibc-langpack-en-2.28-251.el8_10.34.x86_64.rpm, glibc-minimal-langpack-2.28-251.el8_10.34.x86_64.rpm, libnsl-2.28-251.el8_10.34.i686.rpm, libnsl-2.28-251.el8_10.34.x86_64.rpm
CVE-2024-33601	glibc-2.28-251.el8_10.34.i686.rpm, glibc-2.28-251.el8_10.34.x86_64.rpm, glibc-common-2.28-251.el8_10.34.x86_64.rpm, glibc-devel-2.28-251.el8_10.34.x86_64.rpm, glibc-gconv-extra-2.28-251.el8_10.34.i686.rpm, glibc-gconv-extra-2.28-251.el8_10.34.x86_64.rpm, glibc-headers-2.28-251.el8_10.34.x86_64.rpm, glibc-langpack-en-2.28-251.el8_10.34.x86_64.rpm, glibc-minimal-langpack-2.28-251.el8_10.34.x86_64.rpm, libnsl-2.28-251.el8_10.34.i686.rpm, libnsl-2.28-251.el8_10.34.x86_64.rpm
CVE-2024-33602	glibc-2.28-251.el8_10.34.i686.rpm, glibc-2.28-251.el8_10.34.x86_64.rpm, glibc-common-2.28-251.el8_10.34.x86_64.rpm, glibc-devel-2.28-251.el8_10.34.x86_64.rpm, glibc-gconv-extra-2.28-251.el8_10.34.i686.rpm, glibc-gconv-extra-2.28-251.el8_10.34.x86_64.rpm, glibc-headers-2.28-251.el8_10.34.x86_64.rpm, glibc-langpack-en-2.28-251.el8_10.34.x86_64.rpm, glibc-minimal-langpack-2.28-251.el8_10.34.x86_64.rpm, libnsl-2.28-251.el8_10.34.i686.rpm, libnsl-2.28-251.el8_10.34.x86_64.rpm
CVE-2024-33621	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-35235	cups-libs-2.2.6-67.el8_10.x86_64.rpm
CVE-2024-35789	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-35790	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-35801	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-35807	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-35809	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-35810	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-35814	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-35823	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-35824	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-35835	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-35838	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-35839	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-35845	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm

[illegible]

CVE-2024-36017	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-36020	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-36025	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-36270	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-36286	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-36489	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-36883	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-36886	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-36889	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-36896	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-36901	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-36902	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-36904	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-36905	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-36917	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-36919	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-36920	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-36921	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-36922	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-36924	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-36927	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-36929	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-36933	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-36939	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-36940	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-36941	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-36945	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-36950	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-36952	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-36953	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-36954	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-36960	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-36971	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-36978	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-36979	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-37356	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-38538	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-38540	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-38541	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-38555	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-38558	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-38559	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm

[illegible]

CVE-2024-40978	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-40983	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-40984	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-40988	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-40989	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-40995	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-40997	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-40998	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-41005	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-41007	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-41008	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-41009	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-41012	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-41013	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-41014	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-41023	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-41035	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-41038	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-41039	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-41040	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-41041	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-41042	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-41044	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-41055	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-41056	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-41060	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-41064	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-41065	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-41066	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-41071	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-41073	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-41076	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-41090	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-41091	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-41092	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-41093	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-41097	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-42070	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-42079	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-42084	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-42090	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-42094	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm

CVE-2024-42096	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-42114	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-42124	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-42131	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-42152	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-42154	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-42225	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-42226	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-42228	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-42237	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-42238	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-42240	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-42244	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-42246	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-42265	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-42284	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-42285	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-42292	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-42301	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-42322	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-43830	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-43842	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-43854	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-43871	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-43880	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-43889	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-43892	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-44932	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-44935	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-44964	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-44970	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-44989	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-44990	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-45018	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-46695	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-46717	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-46826	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-46858	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-47175	cups-libs-2.2.6-67.el8_10.x86_64.rpm
CVE-2024-47668	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-47696	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-49949	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm

CVE-2024-50082	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-50099	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-50110	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-50138	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-50142	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-50154	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-50192	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-50256	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-50264	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-50274	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-50275	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-50301	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-50302	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-53064	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-53088	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-53095	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-53104	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-53122	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-53141	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-53150	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-53179	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-53197	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-53241	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-54680	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-5535	openssl-1.1.1k-15.el8_6.x86_64.rpm, openssl-devel-1.1.1k-15.el8_6.x86_64.rpm, openssl-libs-1.1.1k-15.el8_6.i686.rpm, openssl-libs-1.1.1k-15.el8_6.x86_64.rpm
CVE-2024-56644	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-57807	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-57980	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-58002	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2024-58057	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-0395	glibc-2.28-251.el8_10.34.i686.rpm, glibc-2.28-251.el8_10.34.x86_64.rpm, glibc-common-2.28-251.el8_10.34.x86_64.rpm, glibc-devel-2.28-251.el8_10.34.x86_64.rpm, glibc-gconv-extra-2.28-251.el8_10.34.i686.rpm, glibc-gconv-extra-2.28-251.el8_10.34.x86_64.rpm, glibc-headers-2.28-251.el8_10.34.x86_64.rpm, glibc-langpack-en-2.28-251.el8_10.34.x86_64.rpm, glibc-minimal-langpack-2.28-251.el8_10.34.x86_64.rpm, libnsl-2.28-251.el8_10.34.i686.rpm, libnsl-2.28-251.el8_10.34.x86_64.rpm

CVE-2025-0938	platform-python-3.6.8-76.el8_10.x86_64.rpm, python3-libs-3.6.8-76.el8_10.x86_64.rpm
CVE-2025-10158	rsync-3.1.3-25.el8_10.x86_64.rpm
CVE-2025-12084	platform-python-3.6.8-76.el8_10.x86_64.rpm, python3-libs-3.6.8-76.el8_10.x86_64.rpm, python3.11-3.11.13-7.el8_10.x86_64.rpm, python3.11-devel-3.11.13-7.el8_10.x86_64.rpm, python3.11-libs-3.11.13-7.el8_10.x86_64.rpm, python3.12-3.12.13-2.el8_10.x86_64.rpm, python3.12-devel-3.12.13-2.el8_10.x86_64.rpm, python3.12-libs-3.12.13-2.el8_10.x86_64.rpm
CVE-2025-13601	glib2-2.56.4-169.el8_10.x86_64.rpm
CVE-2025-13836	python3.11-3.11.13-7.el8_10.x86_64.rpm, python3.11-devel-3.11.13-7.el8_10.x86_64.rpm, python3.11-libs-3.11.13-7.el8_10.x86_64.rpm, python3.12-3.12.13-2.el8_10.x86_64.rpm, python3.12-devel-3.12.13-2.el8_10.x86_64.rpm, python3.12-libs-3.12.13-2.el8_10.x86_64.rpm
CVE-2025-13837	python3.12-3.12.13-2.el8_10.x86_64.rpm, python3.12-devel-3.12.13-2.el8_10.x86_64.rpm, python3.12-libs-3.12.13-2.el8_10.x86_64.rpm
CVE-2025-14087	glib2-2.56.4-169.el8_10.x86_64.rpm
CVE-2025-14104	libblkid-2.32.1-48.el8_10.x86_64.rpm, libfdisk-2.32.1-48.el8_10.x86_64.rpm, libmount-2.32.1-48.el8_10.x86_64.rpm, libsmartcols-2.32.1-48.el8_10.x86_64.rpm, libuuid-2.32.1-48.el8_10.i686.rpm, libuuid-2.32.1-48.el8_10.x86_64.rpm, util-linux-2.32.1-48.el8_10.x86_64.rpm
CVE-2025-14512	glib2-2.56.4-169.el8_10.x86_64.rpm
CVE-2025-14831	gnutls-3.6.16-8.el8_10.5.i686.rpm, gnutls-3.6.16-8.el8_10.5.x86_64.rpm, gnutls-dane-3.6.16-8.el8_10.5.x86_64.rpm, gnutls-utils-3.6.16-8.el8_10.5.x86_64.rpm
CVE-2025-15281	glibc-2.28-251.el8_10.34.i686.rpm, glibc-2.28-251.el8_10.34.x86_64.rpm, glibc-common-2.28-251.el8_10.34.x86_64.rpm, glibc-devel-2.28-251.el8_10.34.x86_64.rpm, glibc-gconv-extra-2.28-251.el8_10.34.i686.rpm, glibc-gconv-extra-2.28-251.el8_10.34.x86_64.rpm, glibc-headers-2.28-251.el8_10.34.x86_64.rpm, glibc-langpack-en-2.28-251.el8_10.34.x86_64.rpm, glibc-minimal-langpack-2.28-251.el8_10.34.x86_64.rpm, libnsl-2.28-251.el8_10.34.i686.rpm, libnsl-2.28-251.el8_10.34.x86_64.rpm
CVE-2025-15282	python3.12-3.12.13-2.el8_10.x86_64.rpm, python3.12-devel-3.12.13-2.el8_10.x86_64.rpm, python3.12-libs-3.12.13-2.el8_10.x86_64.rpm
CVE-2025-15366	platform-python-3.6.8-76.el8_10.x86_64.rpm, python3-libs-3.6.8-76.el8_10.x86_64.rpm, python3.11-3.11.13-7.el8_10.x86_64.rpm, python3.11-devel-3.11.13-7.el8_10.x86_64.rpm, python3.11-libs-3.11.13-7.el8_10.x86_64.rpm, python3.12-3.12.13-

	2.el8_10.x86_64.rpm, python3.12-devel-3.12.13-2.el8_10.x86_64.rpm, python3.12-libs-3.12.13-2.el8_10.x86_64.rpm
CVE-2025-15367	platform-python-3.6.8-76.el8_10.x86_64.rpm, python3-libs-3.6.8-76.el8_10.x86_64.rpm, python3.11-3.11.13-7.el8_10.x86_64.rpm, python3.11-devel-3.11.13-7.el8_10.x86_64.rpm, python3.11-libs-3.11.13-7.el8_10.x86_64.rpm, python3.12-3.12.13-2.el8_10.x86_64.rpm, python3.12-devel-3.12.13-2.el8_10.x86_64.rpm, python3.12-libs-3.12.13-2.el8_10.x86_64.rpm
CVE-2025-21673	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-21725	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-21727	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-21756	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-21759	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-21764	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-21765	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-21766	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-21785	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-21890	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-21905	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-21919	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-21928	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-21991	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-22004	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-22020	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-22026	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-22058	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-22065	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-22077	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-22097	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-22116	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-23131	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-23150	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-26465	openssh-8.0p1-29.el8_10.x86_64.rpm, openssh-clients-8.0p1-29.el8_10.x86_64.rpm, openssh-server-8.0p1-29.el8_10.x86_64.rpm
CVE-2025-32415	libxml2-2.9.7-21.el8_10.4.x86_64.rpm, libxml2-devel-2.9.7-21.el8_10.4.x86_64.rpm, python3-libxml2-2.9.7-21.el8_10.4.x86_64.rpm
CVE-2025-32462	sudo-1.9.5p2-1.el8_10.5.x86_64.rpm

CVE-2025-32988	gnutls-3.6.16-8.el8_10.5.i686.rpm, gnutls-3.6.16-8.el8_10.5.x86_64.rpm, gnutls-dane-3.6.16-8.el8_10.5.x86_64.rpm, gnutls-utils-3.6.16-8.el8_10.5.x86_64.rpm
CVE-2025-32990	gnutls-3.6.16-8.el8_10.5.i686.rpm, gnutls-3.6.16-8.el8_10.5.x86_64.rpm, gnutls-dane-3.6.16-8.el8_10.5.x86_64.rpm, gnutls-utils-3.6.16-8.el8_10.5.x86_64.rpm
CVE-2025-37738	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-37797	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-37798	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-37890	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-37914	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-37932	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-37953	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-38000	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-38001	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-38022	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-38024	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-38051	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-38052	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-38079	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-38085	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-38086	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-38107	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-38129	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-38159	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-38180	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-38200	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-38211	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-38244	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-38248	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-38250	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-38323	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-38332	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-38350	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-38352	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-38380	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-38392	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-38403	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-38415	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-38449	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-38459	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-38461	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm

CVE-2025-38464	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-38477	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-38498	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-38527	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-38556	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-38718	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-38724	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-38729	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-39697	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-39718	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-39730	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-39751	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-39757	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-39760	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-39817	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-39825	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-39841	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-39849	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-39864	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-39883	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-39898	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-39933	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-39955	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-39968	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-39969	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-39970	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-39971	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-39972	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-39973	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-39993	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-40064	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-40096	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-40135	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-40154	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-40158	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-40168	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-40170	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-40240	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-40248	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-40252	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-40258	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-40269	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm

CVE-2025-40271	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-40277	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-40300	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-40304	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-40322	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-4802	glibc-2.28-251.el8_10.34.i686.rpm, glibc-2.28-251.el8_10.34.x86_64.rpm, glibc-common-2.28-251.el8_10.34.x86_64.rpm, glibc-devel-2.28-251.el8_10.34.x86_64.rpm, glibc-gconv-extra-2.28-251.el8_10.34.i686.rpm, glibc-gconv-extra-2.28-251.el8_10.34.x86_64.rpm, glibc-headers-2.28-251.el8_10.34.x86_64.rpm, glibc-langpack-en-2.28-251.el8_10.34.x86_64.rpm, glibc-minimal-langpack-2.28-251.el8_10.34.x86_64.rpm, libnsl-2.28-251.el8_10.34.i686.rpm, libnsl-2.28-251.el8_10.34.x86_64.rpm
CVE-2025-49794	libxml2-2.9.7-21.el8_10.4.x86_64.rpm, libxml2-devel-2.9.7-21.el8_10.4.x86_64.rpm, python3-libxml2-2.9.7-21.el8_10.4.x86_64.rpm
CVE-2025-49796	libxml2-2.9.7-21.el8_10.4.x86_64.rpm, libxml2-devel-2.9.7-21.el8_10.4.x86_64.rpm, python3-libxml2-2.9.7-21.el8_10.4.x86_64.rpm
CVE-2025-5372	libssh-0.9.6-16.el8_10.x86_64.rpm, libssh-config-0.9.6-16.el8_10.noarch.rpm
CVE-2025-53905	vim-common-8.0.1763-22.el8_10.x86_64.rpm, vim-enhanced-8.0.1763-22.el8_10.x86_64.rpm, vim-filesystem-8.0.1763-22.el8_10.noarch.rpm, vim-minimal-8.0.1763-22.el8_10.x86_64.rpm
CVE-2025-53906	vim-common-8.0.1763-22.el8_10.x86_64.rpm, vim-enhanced-8.0.1763-22.el8_10.x86_64.rpm, vim-filesystem-8.0.1763-22.el8_10.noarch.rpm, vim-minimal-8.0.1763-22.el8_10.x86_64.rpm
CVE-2025-58060	cups-libs-2.2.6-67.el8_10.x86_64.rpm
CVE-2025-58364	cups-libs-2.2.6-67.el8_10.x86_64.rpm
CVE-2025-58436	cups-libs-2.2.6-67.el8_10.x86_64.rpm
CVE-2025-59375	expat-2.5.0-1.el8_10.x86_64.rpm, expat-devel-2.5.0-1.el8_10.x86_64.rpm, python3.12-3.12.13-2.el8_10.x86_64.rpm, python3.12-devel-3.12.13-2.el8_10.x86_64.rpm, python3.12-libs-3.12.13-2.el8_10.x86_64.rpm
CVE-2025-6021	libxml2-2.9.7-21.el8_10.4.x86_64.rpm, libxml2-devel-2.9.7-21.el8_10.4.x86_64.rpm, python3-libxml2-2.9.7-21.el8_10.4.x86_64.rpm
CVE-2025-6075	python3.12-3.12.13-2.el8_10.x86_64.rpm, python3.12-devel-3.12.13-2.el8_10.x86_64.rpm, python3.12-libs-3.12.13-2.el8_10.x86_64.rpm
CVE-2025-6176	brotili-1.0.6-4.el8_10.x86_64.rpm

CVE-2025-61915	cups-libs-2.2.6-67.el8_10.x86_64.rpm
CVE-2025-61984	openssh-8.0p1-29.el8_10.x86_64.rpm, openssh-clients-8.0p1-29.el8_10.x86_64.rpm, openssh-server-8.0p1-29.el8_10.x86_64.rpm
CVE-2025-61985	openssh-8.0p1-29.el8_10.x86_64.rpm, openssh-clients-8.0p1-29.el8_10.x86_64.rpm, openssh-server-8.0p1-29.el8_10.x86_64.rpm
CVE-2025-6395	gnutls-3.6.16-8.el8_10.5.i686.rpm, gnutls-3.6.16-8.el8_10.5.x86_64.rpm, gnutls-dane-3.6.16-8.el8_10.5.x86_64.rpm, gnutls-utils-3.6.16-8.el8_10.5.x86_64.rpm
CVE-2025-64720	libpng-1.6.34-10.el8_10.x86_64.rpm
CVE-2025-65018	libpng-1.6.34-10.el8_10.x86_64.rpm
CVE-2025-66293	libpng-1.6.34-10.el8_10.x86_64.rpm
CVE-2025-68285	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-68301	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-68349	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-68724	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-68741	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-68800	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-68973	gnupg2-2.2.20-4.el8_10.x86_64.rpm
CVE-2025-69419	openssl-1.1.1k-15.el8_6.x86_64.rpm, openssl-devel-1.1.1k-15.el8_6.x86_64.rpm, openssl-libs-1.1.1k-15.el8_6.i686.rpm, openssl-libs-1.1.1k-15.el8_6.x86_64.rpm
CVE-2025-71085	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-71238	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2025-7425	libxml2-2.9.7-21.el8_10.4.x86_64.rpm, libxml2-devel-2.9.7-21.el8_10.4.x86_64.rpm, python3-libxml2-2.9.7-21.el8_10.4.x86_64.rpm
CVE-2025-8058	glibc-2.28-251.el8_10.34.i686.rpm, glibc-2.28-251.el8_10.34.x86_64.rpm, glibc-common-2.28-251.el8_10.34.x86_64.rpm, glibc-devel-2.28-251.el8_10.34.x86_64.rpm, glibc-gconv-extra-2.28-251.el8_10.34.i686.rpm, glibc-gconv-extra-2.28-251.el8_10.34.x86_64.rpm, glibc-headers-2.28-251.el8_10.34.x86_64.rpm, glibc-langpack-en-2.28-251.el8_10.34.x86_64.rpm, glibc-minimal-langpack-2.28-251.el8_10.34.x86_64.rpm, libnsl-2.28-251.el8_10.34.i686.rpm, libnsl-2.28-251.el8_10.34.x86_64.rpm
CVE-2025-8176	libtiff-4.0.9-37.el8_10.x86_64.rpm
CVE-2025-8194	python3.11-3.11.13-7.el8_10.x86_64.rpm, python3.11-devel-3.11.13-7.el8_10.x86_64.rpm, python3.11-libs-3.11.13-7.el8_10.x86_64.rpm
CVE-2025-8291	python3.12-3.12.13-2.el8_10.x86_64.rpm, python3.12-devel-3.12.13-2.el8_10.x86_64.rpm, python3.12-libs-3.12.13-2.el8_10.x86_64.rpm

CVE-2025-9086	curl-7.61.1-34.el8_10.11.x86_64.rpm, libcurl-7.61.1-34.el8_10.11.x86_64.rpm
CVE-2025-9230	openssl-1.1.1k-15.el8_6.x86_64.rpm, openssl-devel-1.1.1k-15.el8_6.x86_64.rpm, openssl-lib-1.1.1k-15.el8_6.i686.rpm, openssl-lib-1.1.1k-15.el8_6.x86_64.rpm
CVE-2025-9714	libxml2-2.9.7-21.el8_10.4.x86_64.rpm, libxml2-devel-2.9.7-21.el8_10.4.x86_64.rpm, python3-libxml2-2.9.7-21.el8_10.4.x86_64.rpm
CVE-2025-9820	gnutls-3.6.16-8.el8_10.5.i686.rpm, gnutls-3.6.16-8.el8_10.5.x86_64.rpm, gnutls-dane-3.6.16-8.el8_10.5.x86_64.rpm, gnutls-utils-3.6.16-8.el8_10.5.x86_64.rpm
CVE-2025-9900	libtiff-4.0.9-37.el8_10.x86_64.rpm
CVE-2026-0672	python3.12-3.12.13-2.el8_10.x86_64.rpm, python3.12-devel-3.12.13-2.el8_10.x86_64.rpm, python3.12-lib-3.12.13-2.el8_10.x86_64.rpm
CVE-2026-0865	platform-python-3.6.8-76.el8_10.x86_64.rpm, python3-lib-3.6.8-76.el8_10.x86_64.rpm, python3.11-3.11.13-7.el8_10.x86_64.rpm, python3.11-devel-3.11.13-7.el8_10.x86_64.rpm, python3.11-lib-3.11.13-7.el8_10.x86_64.rpm, python3.12-3.12.13-2.el8_10.x86_64.rpm, python3.12-devel-3.12.13-2.el8_10.x86_64.rpm, python3.12-lib-3.12.13-2.el8_10.x86_64.rpm
CVE-2026-0915	glibc-2.28-251.el8_10.34.i686.rpm, glibc-2.28-251.el8_10.34.x86_64.rpm, glibc-common-2.28-251.el8_10.34.x86_64.rpm, glibc-devel-2.28-251.el8_10.34.x86_64.rpm, glibc-gconv-extra-2.28-251.el8_10.34.i686.rpm, glibc-gconv-extra-2.28-251.el8_10.34.x86_64.rpm, glibc-headers-2.28-251.el8_10.34.x86_64.rpm, glibc-langpack-en-2.28-251.el8_10.34.x86_64.rpm, glibc-minimal-langpack-2.28-251.el8_10.34.x86_64.rpm, libnsl-2.28-251.el8_10.34.i686.rpm, libnsl-2.28-251.el8_10.34.x86_64.rpm
CVE-2026-1299	platform-python-3.6.8-76.el8_10.x86_64.rpm, python3-lib-3.6.8-76.el8_10.x86_64.rpm, python3.11-3.11.13-7.el8_10.x86_64.rpm, python3.11-devel-3.11.13-7.el8_10.x86_64.rpm, python3.11-lib-3.11.13-7.el8_10.x86_64.rpm, python3.12-3.12.13-2.el8_10.x86_64.rpm, python3.12-devel-3.12.13-2.el8_10.x86_64.rpm, python3.12-lib-3.12.13-2.el8_10.x86_64.rpm
CVE-2026-1502	python3.12-3.12.13-2.el8_10.x86_64.rpm, python3.12-devel-3.12.13-2.el8_10.x86_64.rpm, python3.12-lib-3.12.13-2.el8_10.x86_64.rpm
CVE-2026-22695	libpng-1.6.34-10.el8_10.x86_64.rpm
CVE-2026-22801	libpng-1.6.34-10.el8_10.x86_64.rpm

CVE-2026-2297	python3.12-3.12.13-2.el8_10.x86_64.rpm, python3.12-devel-3.12.13-2.el8_10.x86_64.rpm, python3.12-libs-3.12.13-2.el8_10.x86_64.rpm
CVE-2026-22998	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2026-23001	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2026-23060	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2026-23074	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2026-23097	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2026-23191	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2026-23193	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2026-23204	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2026-23209	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2026-23231	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2026-23401	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2026-25646	libpng-1.6.34-10.el8_10.x86_64.rpm
CVE-2026-25749	vim-common-8.0.1763-22.el8_10.x86_64.rpm, vim-enhanced-8.0.1763-22.el8_10.x86_64.rpm, vim-filessystem-8.0.1763-22.el8_10.noarch.rpm, vim-minimal-8.0.1763-22.el8_10.x86_64.rpm
CVE-2026-27135	libnghttp2-1.33.0-6.el8_10.2.x86_64.rpm
CVE-2026-31402	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2026-31431	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2026-31677	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2026-3497	openssh-8.0p1-29.el8_10.x86_64.rpm, openssh-clients-8.0p1-29.el8_10.x86_64.rpm, openssh-server-8.0p1-29.el8_10.x86_64.rpm
CVE-2026-35385	openssh-8.0p1-29.el8_10.x86_64.rpm, openssh-clients-8.0p1-29.el8_10.x86_64.rpm, openssh-server-8.0p1-29.el8_10.x86_64.rpm
CVE-2026-35386	openssh-8.0p1-29.el8_10.x86_64.rpm, openssh-clients-8.0p1-29.el8_10.x86_64.rpm, openssh-server-8.0p1-29.el8_10.x86_64.rpm
CVE-2026-35387	openssh-8.0p1-29.el8_10.x86_64.rpm, openssh-clients-8.0p1-29.el8_10.x86_64.rpm, openssh-server-8.0p1-29.el8_10.x86_64.rpm
CVE-2026-35388	openssh-8.0p1-29.el8_10.x86_64.rpm, openssh-clients-8.0p1-29.el8_10.x86_64.rpm, openssh-server-8.0p1-29.el8_10.x86_64.rpm
CVE-2026-35414	openssh-8.0p1-29.el8_10.x86_64.rpm, openssh-clients-8.0p1-29.el8_10.x86_64.rpm, openssh-server-8.0p1-29.el8_10.x86_64.rpm
CVE-2026-35535	sudo-1.9.5p2-1.el8_10.5.x86_64.rpm

CVE-2026-3644	python3.12-3.12.13-2.el8_10.x86_64.rpm, python3.12-devel-3.12.13-2.el8_10.x86_64.rpm, python3.12-libs-3.12.13-2.el8_10.x86_64.rpm
CVE-2026-39979	jq-1.6-12.el8_10.x86_64.rpm
CVE-2026-40164	jq-1.6-12.el8_10.x86_64.rpm
CVE-2026-40355	krb5-devel-1.18.2-34.el8_10.x86_64.rpm, krb5-libs-1.18.2-34.el8_10.i686.rpm, krb5-libs-1.18.2-34.el8_10.x86_64.rpm, libkadm5-1.18.2-34.el8_10.x86_64.rpm
CVE-2026-40356	krb5-devel-1.18.2-34.el8_10.x86_64.rpm, krb5-libs-1.18.2-34.el8_10.i686.rpm, krb5-libs-1.18.2-34.el8_10.x86_64.rpm, libkadm5-1.18.2-34.el8_10.x86_64.rpm
CVE-2026-41035	rsync-3.1.3-25.el8_10.x86_64.rpm
CVE-2026-4224	python3.12-3.12.13-2.el8_10.x86_64.rpm, python3.12-devel-3.12.13-2.el8_10.x86_64.rpm, python3.12-libs-3.12.13-2.el8_10.x86_64.rpm
CVE-2026-43284	kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
CVE-2026-4424	libarchive-3.3.3-7.el8_10.x86_64.rpm
CVE-2026-4519	platform-python-3.6.8-76.el8_10.x86_64.rpm, python3-libs-3.6.8-76.el8_10.x86_64.rpm, python3.11-3.11.13-7.el8_10.x86_64.rpm, python3.11-devel-3.11.13-7.el8_10.x86_64.rpm, python3.11-libs-3.11.13-7.el8_10.x86_64.rpm, python3.12-3.12.13-2.el8_10.x86_64.rpm, python3.12-devel-3.12.13-2.el8_10.x86_64.rpm, python3.12-libs-3.12.13-2.el8_10.x86_64.rpm
CVE-2026-4775	libtiff-4.0.9-37.el8_10.x86_64.rpm
CVE-2026-4786	platform-python-3.6.8-76.el8_10.x86_64.rpm, python3-libs-3.6.8-76.el8_10.x86_64.rpm, python3.11-3.11.13-7.el8_10.x86_64.rpm, python3.11-devel-3.11.13-7.el8_10.x86_64.rpm, python3.11-libs-3.11.13-7.el8_10.x86_64.rpm, python3.12-3.12.13-2.el8_10.x86_64.rpm, python3.12-devel-3.12.13-2.el8_10.x86_64.rpm, python3.12-libs-3.12.13-2.el8_10.x86_64.rpm
CVE-2026-4878	libcap-2.48-6.el8_10.1.x86_64.rpm
CVE-2026-5121	libarchive-3.3.3-7.el8_10.x86_64.rpm
CVE-2026-5201	gdk-pixbuf2-2.36.12-8.el8_10.x86_64.rpm, gdk-pixbuf2-modules-2.36.12-8.el8_10.x86_64.rpm
CVE-2026-6100	platform-python-3.6.8-76.el8_10.x86_64.rpm, python3-libs-3.6.8-76.el8_10.x86_64.rpm, python3.11-3.11.13-7.el8_10.x86_64.rpm, python3.11-devel-3.11.13-7.el8_10.x86_64.rpm, python3.11-libs-3.11.13-7.el8_10.x86_64.rpm, python3.12-3.12.13-2.el8_10.x86_64.rpm, python3.12-devel-3.12.13-2.el8_10.x86_64.rpm, python3.12-libs-3.12.13-2.el8_10.x86_64.rpm

3.2 3PP Changes

3.2.1 3PP Changes in WS-OS iso

ws-os-25.12.0-11.iso updated software list.
 chrony-4.5-2.el8_10.x86_64.rpm
 container-selinux-2.229.0-2.module+el8.10.0+24081+a04d358a.noarch.rpm
 dnsmasq-2.79-35.el8_10.x86_64.rpm
 jq-1.6-12.el8_10.x86_64.rpm
 kernel-modules-extra-4.18.0-553.124.1.el8_10.x86_64.rpm
 platform-python-setuptools-39.2.0-9.el8_10.noarch.rpm
 policycoreutils-python-utils-2.9-26.el8_10.noarch.rpm
 python3-audit-3.1.2-1.el8_10.1.x86_64.rpm
 python3-libsemanage-2.9-12.el8_10.x86_64.rpm
 python3-policycoreutils-2.9-26.el8_10.noarch.rpm
 python3-setuptools-39.2.0-9.el8_10.noarch.rpm
 python3.12-3.12.13-2.el8_10.x86_64.rpm
 python3.12-libs-3.12.13-2.el8_10.x86_64.rpm
 python3.12-setuptools-68.2.2-5.el8_10.noarch.rpm
 rng-tools-6.16-2.el8_10.x86_64.rpm
 tar-1.30-11.el8_10.x86_64.rpm
 vim-common-8.0.1763-22.el8_10.3.x86_64.rpm
 vim-enhanced-8.0.1763-22.el8_10.3.x86_64.rpm
 vim-filessystem-8.0.1763-22.el8_10.3.noarch.rpm
 wget-1.19.5-12.el8_10.x86_64.rpm

3.2.2 3PP changes on RedHat Containers (upgraded on containers only)

aopalliance-1.0-20.module+el8.8.0+18043+17ecf8f0.noarch.rpm
 apache-commons-io-2.11.0-3.module+el8.10.0+21301+657f54a3.noarch.rpm
 apr-1.6.3-12.el8.x86_64.rpm
 audit-3.1.2-1.el8_10.1.x86_64.rpm
 audit-libs-3.1.2-1.el8_10.1.x86_64.rpm
 autoconf-2.69-29.el8_10.1.noarch.rpm
 avahi-libs-0.7-27.el8_10.1.x86_64.rpm
 bash-4.4.20-6.el8_10.x86_64.rpm
 bind-libs-9.11.36-14.el8_10.x86_64.rpm
 bind-libs-lite-9.11.36-14.el8_10.x86_64.rpm
 bind-license-9.11.36-14.el8_10.noarch.rpm
 bind-utils-9.11.36-14.el8_10.x86_64.rpm
 binutils-2.30-125.el8_10.x86_64.rpm
 binutils-2.30-128.el8_10.x86_64.rpm

bpftool-4.18.0-553.50.1.el8_10.x86_64.rpm
 brotli-1.0.6-4.el8_10.x86_64.rpm
 buildah-1.33.7-2.module+el8.10.0+21962+8143777b.x86_64.rpm
 bzip2-1.0.6-28.el8_10.x86_64.rpm
 bzip2-devel-1.0.6-28.el8_10.x86_64.rpm
 bzip2-libs-1.0.6-28.el8_10.x86_64.rpm
 c-ares-1.13.0-11.el8_10.x86_64.rpm
 ca-certificates-2024.2.69_v8.0.303-80.0.el8_10.noarch.rpm
 ca-certificates-2025.2.80_v9.0.304-80.2.el8_10.noarch.rpm
 checkpolicy-2.9-1.el8.x86_64.rpm
 cheese-3.28.0-4.el8_6.x86_64.rpm
 cheese-libs-3.28.0-4.el8_6.x86_64.rpm
 chrony-4.5-2.el8_10.x86_64.rpm
 clang-17.0.6-1.module+el8.10.0+20808+e12784c0.x86_64.rpm
 clang-devel-17.0.6-1.module+el8.10.0+20808+e12784c0.x86_64.rpm
 clang-libs-17.0.6-1.module+el8.10.0+20808+e12784c0.x86_64.rpm
 clang-resource-filesystem-17.0.6-1.module+el8.10.0+20808+e12784c0.noarch.rpm
 clang-tools-extra-17.0.6-1.module+el8.10.0+20808+e12784c0.x86_64.rpm
 clang-tools-extra-devel-17.0.6-1.module+el8.10.0+20808+e12784c0.x86_64.rpm
 cockpit-310.4-1.el8_10.x86_64.rpm
 cockpit-bridge-310.4-1.el8_10.x86_64.rpm
 cockpit-podman-84.1-1.module+el8.10.0+21962+8143777b.noarch.rpm
 cockpit-system-310.4-1.el8_10.noarch.rpm
 cockpit-ws-310.4-1.el8_10.x86_64.rpm
 compat-openssl10-1.0.2o-4.el8_10.1.i686.rpm
 compat-openssl10-1.0.2o-4.el8_10.1.x86_64.rpm
 compiler-rt-17.0.6-1.module+el8.10.0+20808+e12784c0.x86_64.rpm
 common-2.1.10-1.module+el8.10.0+21962+8143777b.x86_64.rpm
 container-selinux-2.229.0-2.module+el8.10.0+22931+799fd806.noarch.rpm
 container-selinux-2.229.0-2.module+el8.10.0+24081+a04d358a.noarch.rpm
 containernetworking-plugins-1.4.0-5.module+el8.10.0+22931+799fd806.x86_64.rpm
 containers-common-1-82.module+el8.10.0+22931+799fd806.x86_64.rpm
 coreutils-8.30-17.el8_10.x86_64.rpm
 coreutils-common-8.30-17.el8_10.x86_64.rpm
 cpp-8.5.0-26.el8_10.x86_64.rpm
 cpp-8.5.0-28.el8_10.x86_64.rpm
 criu-3.18-5.module+el8.10.0+21962+8143777b.x86_64.rpm
 cups-libs-2.2.6-62.el8_10.x86_64.rpm
 cups-libs-2.2.6-63.el8_10.x86_64.rpm
 cups-libs-2.2.6-67.el8_10.x86_64.rpm
 curl-7.61.1-34.el8_10.11.x86_64.rpm
 curl-7.61.1-34.el8_10.2.x86_64.rpm
 dbus-1.12.8-27.el8_10.x86_64.rpm

dbus-1.12.8-28.el8_10.x86_64.rpm
 dbus-common-1.12.8-27.el8_10.noarch.rpm
 dbus-common-1.12.8-28.el8_10.noarch.rpm
 dbus-daemon-1.12.8-27.el8_10.x86_64.rpm
 dbus-daemon-1.12.8-28.el8_10.x86_64.rpm
 dbus-libs-1.12.8-27.el8_10.x86_64.rpm
 dbus-libs-1.12.8-28.el8_10.x86_64.rpm
 dbus-tools-1.12.8-27.el8_10.x86_64.rpm
 dbus-tools-1.12.8-28.el8_10.x86_64.rpm
 device-mapper-1.02.181-15.el8_10.3.x86_64.rpm
 device-mapper-event-1.02.181-15.el8_10.3.x86_64.rpm
 device-mapper-event-libs-1.02.181-15.el8_10.3.x86_64.rpm
 device-mapper-libs-1.02.181-15.el8_10.3.x86_64.rpm
 diffutils-3.6-6.el8.x86_64.rpm
 dnf-4.7.0-21.el8_10.noarch.rpm
 dnf-data-4.7.0-21.el8_10.noarch.rpm
 dnf-plugin-subscription-manager-1.28.44-1.el8_10.x86_64.rpm
 dnsmasq-2.79-35.el8_10.x86_64.rpm
 docker-ce-cli-28.5.1-1.el8.x86_64.rpm
 dracut-049-239.git20251127.el8_10.x86_64.rpm
 dracut-config-rescue-049-239.git20251127.el8_10.x86_64.rpm
 dracut-network-049-239.git20251127.el8_10.x86_64.rpm
 dracut-squash-049-239.git20251127.el8_10.x86_64.rpm
 e2fsprogs-1.45.6-7.el8_10.x86_64.rpm
 e2fsprogs-libs-1.45.6-7.el8_10.x86_64.rpm
 elfutils-debuginfod-client-0.188-3.el8.x86_64.rpm
 emacs-filesystem-26.1-15.el8_10.noarch.rpm
 environment-modules-4.5.2-4.el8.x86_64.rpm
 expat-2.2.5-16.el8_10.x86_64.rpm
 expat-2.2.5-17.el8_10.x86_64.rpm
 expat-2.5.0-1.el8_10.x86_64.rpm
 expat-devel-2.2.5-17.el8_10.x86_64.rpm
 expat-devel-2.5.0-1.el8_10.x86_64.rpm
 file-5.33-27.el8_10.x86_64.rpm
 file-libs-5.33-27.el8_10.x86_64.rpm
 findutils-4.6.0-24.el8_10.x86_64.rpm
 firefox-115.12.0-1.el8_10.x86_64.rpm
 firewalld-0.9.11-10.el8_10.noarch.rpm
 firewalld-filesystem-0.9.11-10.el8_10.noarch.rpm
 flatpak-1.12.9-1.el8_10.x86_64.rpm
 flatpak-libs-1.12.9-1.el8_10.x86_64.rpm
 flatpak-selinux-1.12.9-1.el8_10.noarch.rpm
 flatpak-session-helper-1.12.9-1.el8_10.x86_64.rpm

freetype-2.9.1-10.el8_10.x86_64.rpm
freetype-devel-2.9.1-10.el8_10.x86_64.rpm
fuse-overlayfs-1.13-1.module+el8.10.0+22931+799fd806.x86_64.rpm
fuse-overlayfs-1.13-1.module+el8.10.0+24081+a04d358a.x86_64.rpm
gcc-8.5.0-26.el8_10.x86_64.rpm
gcc-8.5.0-28.el8_10.x86_64.rpm
gcc-c++-8.5.0-26.el8_10.x86_64.rpm
gcc-c++-8.5.0-28.el8_10.x86_64.rpm
gcc-plugin-annobin-8.5.0-26.el8_10.x86_64.rpm
gcc-plugin-annobin-8.5.0-28.el8_10.x86_64.rpm
gcc-toolset-13-binutils-2.40-21.el8.x86_64.rpm
gcc-toolset-13-binutils-gold-2.40-21.el8.x86_64.rpm
gcc-toolset-13-gcc-13.2.1-6.2.el8.x86_64.rpm
gcc-toolset-13-gcc-c++-13.2.1-6.2.el8.x86_64.rpm
gcc-toolset-13-libstdc++-devel-13.2.1-6.2.el8.x86_64.rpm
gcc-toolset-13-runtime-13.0-2.el8.x86_64.rpm
gdk-pixbuf2-2.36.12-6.el8_10.x86_64.rpm
gdk-pixbuf2-2.36.12-7.el8_10.x86_64.rpm
gdk-pixbuf2-2.36.12-8.el8_10.x86_64.rpm
gdk-pixbuf2-devel-2.36.12-7.el8_10.x86_64.rpm
gdk-pixbuf2-modules-2.36.12-6.el8_10.x86_64.rpm
gdk-pixbuf2-modules-2.36.12-7.el8_10.x86_64.rpm
gdk-pixbuf2-modules-2.36.12-8.el8_10.x86_64.rpm
git-2.43.7-1.el8_10.x86_64.rpm
git-core-2.43.7-1.el8_10.x86_64.rpm
git-core-doc-2.43.7-1.el8_10.noarch.rpm
glib2-2.56.4-166.el8_10.x86_64.rpm
glib2-2.56.4-168.el8_10.x86_64.rpm
glib2-2.56.4-169.el8_10.x86_64.rpm
glibc-2.28-251.el8_10.2.i686.rpm
glibc-2.28-251.el8_10.2.x86_64.rpm
glibc-2.28-251.el8_10.25.i686.rpm
glibc-2.28-251.el8_10.25.x86_64.rpm
glibc-2.28-251.el8_10.27.x86_64.rpm
glibc-2.28-251.el8_10.31.i686.rpm
glibc-2.28-251.el8_10.31.x86_64.rpm
glibc-2.28-251.el8_10.34.i686.rpm
glibc-2.28-251.el8_10.34.x86_64.rpm
glibc-all-langpacks-2.28-251.el8_10.2.x86_64.rpm
glibc-all-langpacks-2.28-251.el8_10.22.x86_64.rpm
glibc-all-langpacks-2.28-251.el8_10.31.x86_64.rpm
glibc-common-2.28-251.el8_10.2.x86_64.rpm
glibc-common-2.28-251.el8_10.25.x86_64.rpm

glibc-common-2.28-251.el8_10.27.x86_64.rpm
glibc-common-2.28-251.el8_10.31.x86_64.rpm
glibc-common-2.28-251.el8_10.34.x86_64.rpm
glibc-devel-2.28-251.el8_10.2.i686.rpm
glibc-devel-2.28-251.el8_10.2.x86_64.rpm
glibc-devel-2.28-251.el8_10.25.x86_64.rpm
glibc-devel-2.28-251.el8_10.31.x86_64.rpm
glibc-devel-2.28-251.el8_10.34.x86_64.rpm
glibc-gconv-extra-2.28-251.el8_10.2.i686.rpm
glibc-gconv-extra-2.28-251.el8_10.2.x86_64.rpm
glibc-gconv-extra-2.28-251.el8_10.25.i686.rpm
glibc-gconv-extra-2.28-251.el8_10.25.x86_64.rpm
glibc-gconv-extra-2.28-251.el8_10.27.x86_64.rpm
glibc-gconv-extra-2.28-251.el8_10.31.i686.rpm
glibc-gconv-extra-2.28-251.el8_10.31.x86_64.rpm
glibc-gconv-extra-2.28-251.el8_10.34.i686.rpm
glibc-gconv-extra-2.28-251.el8_10.34.x86_64.rpm
glibc-headers-2.28-251.el8_10.2.i686.rpm
glibc-headers-2.28-251.el8_10.2.x86_64.rpm
glibc-headers-2.28-251.el8_10.25.x86_64.rpm
glibc-headers-2.28-251.el8_10.31.x86_64.rpm
glibc-headers-2.28-251.el8_10.34.x86_64.rpm
glibc-langpack-en-2.28-251.el8_10.2.x86_64.rpm
glibc-langpack-en-2.28-251.el8_10.25.x86_64.rpm
glibc-langpack-en-2.28-251.el8_10.27.x86_64.rpm
glibc-langpack-en-2.28-251.el8_10.31.x86_64.rpm
glibc-langpack-en-2.28-251.el8_10.34.x86_64.rpm
glibc-minimal-langpack-2.28-251.el8_10.2.x86_64.rpm
glibc-minimal-langpack-2.28-251.el8_10.25.x86_64.rpm
glibc-minimal-langpack-2.28-251.el8_10.31.x86_64.rpm
glibc-minimal-langpack-2.28-251.el8_10.34.x86_64.rpm
gnupg2-2.2.20-4.el8_10.x86_64.rpm
gnupg2-smime-2.2.20-4.el8_10.x86_64.rpm
gnutls-3.6.16-8.el8_10.3.i686.rpm
gnutls-3.6.16-8.el8_10.3.x86_64.rpm
gnutls-3.6.16-8.el8_10.4.x86_64.rpm
gnutls-3.6.16-8.el8_10.5.i686.rpm
gnutls-3.6.16-8.el8_10.5.x86_64.rpm
gnutls-dane-3.6.16-8.el8_10.3.x86_64.rpm
gnutls-dane-3.6.16-8.el8_10.4.x86_64.rpm
gnutls-dane-3.6.16-8.el8_10.5.x86_64.rpm
gnutls-utils-3.6.16-8.el8_10.3.x86_64.rpm
gnutls-utils-3.6.16-8.el8_10.4.x86_64.rpm

gnutls-utils-3.6.16-8.el8_10.5.x86_64.rpm
 gpgme-1.13.1-11.el8.i686.rpm
 gpgme-1.13.1-11.el8.x86_64.rpm
 gpgmepp-1.13.1-11.el8.i686.rpm
 gpgmepp-1.13.1-11.el8.x86_64.rpm
 grub2-common-2.02-167.el8_10.noarch.rpm
 grub2-common-2.02-169.el8_10.noarch.rpm
 grub2-common-2.02-170.el8_10.1.noarch.rpm
 grub2-pc-2.02-170.el8_10.1.x86_64.rpm
 grub2-pc-modules-2.02-170.el8_10.1.noarch.rpm
 grub2-tools-2.02-167.el8_10.x86_64.rpm
 grub2-tools-2.02-170.el8_10.1.x86_64.rpm
 grub2-tools-efi-2.02-170.el8_10.1.x86_64.rpm
 grub2-tools-extra-2.02-170.el8_10.1.x86_64.rpm
 grub2-tools-minimal-2.02-167.el8_10.x86_64.rpm
 grub2-tools-minimal-2.02-170.el8_10.1.x86_64.rpm
 gtk-update-icon-cache-3.22.30-12.el8_10.x86_64.rpm
 gtk3-3.22.30-12.el8_10.x86_64.rpm
 hyperv-daemons-0-0.34.20180415git.el8_7.x86_64.rpm
 hyperv-daemons-license-0-0.34.20180415git.el8_7.noarch.rpm
 hypervfcopyd-0-0.34.20180415git.el8_7.x86_64.rpm
 hypervkvpd-0-0.34.20180415git.el8_7.x86_64.rpm
 hypervvssd-0-0.34.20180415git.el8_7.x86_64.rpm
 ibus-1.5.19-14.el8_5.x86_64.rpm
 ibus-gtk2-1.5.19-14.el8_5.x86_64.rpm
 ibus-gtk3-1.5.19-14.el8_5.x86_64.rpm
 ibus-libs-1.5.19-14.el8_5.x86_64.rpm
 ibus-setup-1.5.19-14.el8_5.noarch.rpm
 initscripts-10.00.19-1.el8_10.x86_64.rpm
 iscsi-initiator-utils-6.2.1.4-8.git095f59c.el8_8.x86_64.rpm
 iscsi-initiator-utils-iscsiuio-6.2.1.4-8.git095f59c.el8_8.x86_64.rpm
 iwl100-firmware-39.31.5.1-135.el8_10.1.noarch.rpm
 iwl100-firmware-39.31.5.1-138.el8_10.1.noarch.rpm
 iwl1000-firmware-39.31.5.1-135.el8_10.1.noarch.rpm
 iwl1000-firmware-39.31.5.1-138.el8_10.1.noarch.rpm
 iwl105-firmware-18.168.6.1-135.el8_10.1.noarch.rpm
 iwl105-firmware-18.168.6.1-138.el8_10.1.noarch.rpm
 iwl135-firmware-18.168.6.1-135.el8_10.1.noarch.rpm
 iwl135-firmware-18.168.6.1-138.el8_10.1.noarch.rpm
 iwl2000-firmware-18.168.6.1-135.el8_10.1.noarch.rpm
 iwl2000-firmware-18.168.6.1-138.el8_10.1.noarch.rpm
 iwl2030-firmware-18.168.6.1-135.el8_10.1.noarch.rpm
 iwl2030-firmware-18.168.6.1-138.el8_10.1.noarch.rpm

iwl3160-firmware-25.30.13.0-135.el8_10.1.noarch.rpm
 iwl3160-firmware-25.30.13.0-138.el8_10.1.noarch.rpm
 iwl5000-firmware-8.83.5.1_1-135.el8_10.1.noarch.rpm
 iwl5000-firmware-8.83.5.1_1-138.el8_10.1.noarch.rpm
 iwl5150-firmware-8.24.2.2-135.el8_10.1.noarch.rpm
 iwl5150-firmware-8.24.2.2-138.el8_10.1.noarch.rpm
 iwl6000-firmware-9.221.4.1-135.el8_10.1.noarch.rpm
 iwl6000-firmware-9.221.4.1-138.el8_10.1.noarch.rpm
 iwl6000g2a-firmware-18.168.6.1-135.el8_10.1.noarch.rpm
 iwl6000g2a-firmware-18.168.6.1-138.el8_10.1.noarch.rpm
 iwl6050-firmware-41.28.5.1-135.el8_10.1.noarch.rpm
 iwl6050-firmware-41.28.5.1-138.el8_10.1.noarch.rpm
 iwl7260-firmware-25.30.13.0-135.el8_10.1.noarch.rpm
 iwl7260-firmware-25.30.13.0-138.el8_10.1.noarch.rpm
 jasper-libs-2.0.14-6.el8_10.x86_64.rpm
 java-1.8.0-openjdk-1.8.0.442.b06-2.el8.x86_64.rpm
 java-1.8.0-openjdk-1.8.0.462.b08-2.el8.x86_64.rpm
 java-1.8.0-openjdk-1.8.0.482.b08-1.el8.x86_64.rpm
 java-1.8.0-openjdk-1.8.0.492.b09-1.el8.x86_64.rpm
 java-1.8.0-openjdk-devel-1.8.0.442.b06-2.el8.x86_64.rpm
 java-1.8.0-openjdk-devel-1.8.0.462.b08-2.el8.x86_64.rpm
 java-1.8.0-openjdk-devel-1.8.0.482.b08-1.el8.x86_64.rpm
 java-1.8.0-openjdk-devel-1.8.0.492.b09-1.el8.x86_64.rpm
 java-1.8.0-openjdk-headless-1.8.0.442.b06-2.el8.x86_64.rpm
 java-1.8.0-openjdk-headless-1.8.0.462.b08-2.el8.x86_64.rpm
 java-1.8.0-openjdk-headless-1.8.0.482.b08-1.el8.x86_64.rpm
 java-1.8.0-openjdk-headless-1.8.0.492.b09-1.el8.x86_64.rpm
 java-11-openjdk-11.0.25.0.9-2.el8.x86_64.rpm
 java-11-openjdk-devel-11.0.25.0.9-2.el8.x86_64.rpm
 java-11-openjdk-headless-11.0.25.0.9-2.el8.x86_64.rpm
 java-17-openjdk-17.0.14.0.7-3.el8.x86_64.rpm
 java-17-openjdk-17.0.16.0.8-2.el8.x86_64.rpm
 java-17-openjdk-17.0.18.0.8-1.el8.x86_64.rpm
 java-17-openjdk-demo-17.0.16.0.8-2.el8.x86_64.rpm
 java-17-openjdk-demo-17.0.18.0.8-1.el8.x86_64.rpm
 java-17-openjdk-devel-17.0.14.0.7-3.el8.x86_64.rpm
 java-17-openjdk-devel-17.0.16.0.8-2.el8.x86_64.rpm
 java-17-openjdk-devel-17.0.18.0.8-1.el8.x86_64.rpm
 java-17-openjdk-headless-17.0.14.0.7-3.el8.x86_64.rpm
 java-17-openjdk-headless-17.0.16.0.8-2.el8.x86_64.rpm
 java-17-openjdk-headless-17.0.18.0.8-1.el8.x86_64.rpm
 java-17-openjdk-javadoc-17.0.16.0.8-2.el8.x86_64.rpm
 java-17-openjdk-javadoc-17.0.18.0.8-1.el8.x86_64.rpm

java-17-openjdk-javadoc-zip-17.0.16.0.8-2.el8.x86_64.rpm
java-17-openjdk-jmods-17.0.16.0.8-2.el8.x86_64.rpm
java-17-openjdk-src-17.0.16.0.8-2.el8.x86_64.rpm
java-17-openjdk-static-libs-17.0.16.0.8-2.el8.x86_64.rpm
jq-1.6-11.el8_10.x86_64.rpm
jq-1.6-12.el8_10.x86_64.rpm
jq-1.6-9.el8_10.x86_64.rpm
kernel-4.18.0-553.104.1.el8_10.x86_64.rpm
kernel-4.18.0-553.111.1.el8_10.x86_64.rpm
kernel-4.18.0-553.117.1.el8_10.x86_64.rpm
kernel-4.18.0-553.123.1.el8_10.x86_64.rpm
kernel-4.18.0-553.124.1.el8_10.x86_64.rpm
kernel-4.18.0-553.50.1.el8_10.x86_64.rpm
kernel-core-4.18.0-553.111.1.el8_10.x86_64.rpm
kernel-core-4.18.0-553.117.1.el8_10.x86_64.rpm
kernel-core-4.18.0-553.123.1.el8_10.x86_64.rpm
kernel-core-4.18.0-553.124.1.el8_10.x86_64.rpm
kernel-core-4.18.0-553.50.1.el8_10.x86_64.rpm
kernel-devel-4.18.0-553.111.1.el8_10.x86_64.rpm
kernel-devel-4.18.0-553.117.1.el8_10.x86_64.rpm
kernel-devel-4.18.0-553.123.1.el8_10.x86_64.rpm
kernel-devel-4.18.0-553.124.1.el8_10.x86_64.rpm
kernel-headers-4.18.0-553.111.1.el8_10.x86_64.rpm
kernel-headers-4.18.0-553.117.1.el8_10.x86_64.rpm
kernel-headers-4.18.0-553.123.1.el8_10.x86_64.rpm
kernel-headers-4.18.0-553.124.1.el8_10.x86_64.rpm
kernel-headers-4.18.0-553.50.1.el8_10.x86_64.rpm
kernel-headers-4.18.0-553.72.1.el8_10.x86_64.rpm
kernel-headers-4.18.0-553.79.1.el8_10.x86_64.rpm
kernel-modules-4.18.0-553.111.1.el8_10.x86_64.rpm
kernel-modules-4.18.0-553.117.1.el8_10.x86_64.rpm
kernel-modules-4.18.0-553.123.1.el8_10.x86_64.rpm
kernel-modules-4.18.0-553.124.1.el8_10.x86_64.rpm
kernel-modules-4.18.0-553.50.1.el8_10.x86_64.rpm
kernel-tools-4.18.0-553.111.1.el8_10.x86_64.rpm
kernel-tools-4.18.0-553.117.1.el8_10.x86_64.rpm
kernel-tools-4.18.0-553.123.1.el8_10.x86_64.rpm
kernel-tools-4.18.0-553.124.1.el8_10.x86_64.rpm
kernel-tools-4.18.0-553.50.1.el8_10.x86_64.rpm
kernel-tools-libs-4.18.0-553.111.1.el8_10.x86_64.rpm
kernel-tools-libs-4.18.0-553.117.1.el8_10.x86_64.rpm
kernel-tools-libs-4.18.0-553.123.1.el8_10.x86_64.rpm
kernel-tools-libs-4.18.0-553.124.1.el8_10.x86_64.rpm

kernel-tools-libs-4.18.0-553.50.1.el8_10.x86_64.rpm
 kexec-tools-2.0.26-14.el8_10.3.x86_64.rpm
 keyutils-libs-1.5.10-9.el8.i686.rpm
 keyutils-libs-devel-1.5.10-9.el8.x86_64.rpm
 kmod-kvdo-6.2.8.7-94.el8.x86_64.rpm
 kpartx-0.8.4-42.el8_10.x86_64.rpm
 kpartx-0.8.4-44.el8_10.x86_64.rpm
 krb5-devel-1.18.2-31.el8_10.x86_64.rpm
 krb5-devel-1.18.2-32.el8_10.i686.rpm
 krb5-devel-1.18.2-32.el8_10.x86_64.rpm
 krb5-devel-1.18.2-33.el8_10.i686.rpm
 krb5-devel-1.18.2-33.el8_10.x86_64.rpm
 krb5-devel-1.18.2-34.el8_10.x86_64.rpm
 krb5-libs-1.18.2-31.el8_10.i686.rpm
 krb5-libs-1.18.2-31.el8_10.x86_64.rpm
 krb5-libs-1.18.2-32.el8_10.i686.rpm
 krb5-libs-1.18.2-32.el8_10.x86_64.rpm
 krb5-libs-1.18.2-33.el8_10.i686.rpm
 krb5-libs-1.18.2-33.el8_10.x86_64.rpm
 krb5-libs-1.18.2-34.el8_10.i686.rpm
 krb5-libs-1.18.2-34.el8_10.x86_64.rpm
 krb5-server-1.18.2-31.el8_10.x86_64.rpm
 krb5-server-1.18.2-32.el8_10.i686.rpm
 krb5-server-1.18.2-32.el8_10.x86_64.rpm
 krb5-server-1.18.2-33.el8_10.i686.rpm
 krb5-server-1.18.2-33.el8_10.x86_64.rpm
 krb5-server-1.18.2-34.el8_10.i686.rpm
 krb5-server-1.18.2-34.el8_10.x86_64.rpm
 leapp-0.19.0-1.el8_10.noarch.rpm
 leapp-deps-0.19.0-1.el8_10.noarch.rpm
 leapp-upgrade-el8toel9-0.22.0-1.el8_10.noarch.rpm
 leapp-upgrade-el8toel9-deps-0.22.0-1.el8_10.noarch.rpm
 less-530-3.el8_10.x86_64.rpm
 libarchive-3.3.3-6.el8_10.x86_64.rpm
 libarchive-3.3.3-7.el8_10.x86_64.rpm
 libblkid-2.32.1-48.el8_10.x86_64.rpm
 libcap-2.48-6.el8_10.1.x86_64.rpm
 libcom_err-1.45.6-5.el8.i686.rpm
 libcom_err-1.45.6-7.el8_10.i686.rpm
 libcom_err-1.45.6-7.el8_10.x86_64.rpm
 libcom_err-devel-1.45.6-5.el8.x86_64.rpm
 libcom_err-devel-1.45.6-7.el8_10.x86_64.rpm
 libcurl-7.61.1-34.el8_10.11.x86_64.rpm

libcurl-7.61.1-34.el8_10.2.x86_64.rpm
 libdnf-0.63.0-20.el8_10.x86_64.rpm
 libdnf-0.63.0-21.el8_10.x86_64.rpm
 libev-4.24-6.el8.x86_64.rpm
 libfdisk-2.32.1-48.el8_10.x86_64.rpm
 libgcc-8.5.0-26.el8_10.i686.rpm
 libgcc-8.5.0-26.el8_10.x86_64.rpm
 libgcc-8.5.0-28.el8_10.i686.rpm
 libgcc-8.5.0-28.el8_10.x86_64.rpm
 libgomp-8.5.0-26.el8_10.i686.rpm
 libgomp-8.5.0-26.el8_10.x86_64.rpm
 libgomp-8.5.0-28.el8_10.i686.rpm
 libgomp-8.5.0-28.el8_10.x86_64.rpm
 libgomp-offload-nvptx-8.5.0-26.el8_10.x86_64.rpm
 libgs-9.27-17.el8_10.x86_64.rpm
 libicu-60.3-2.el8_1.x86_64.rpm
 libicu-devel-60.3-2.el8_1.x86_64.rpm
 libipa_hbac-2.9.4-3.el8_10.x86_64.rpm
 libjpeg-turbo-1.5.3-14.el8_10.x86_64.rpm
 libkadm5-1.18.2-31.el8_10.i686.rpm
 libkadm5-1.18.2-31.el8_10.x86_64.rpm
 libkadm5-1.18.2-32.el8_10.i686.rpm
 libkadm5-1.18.2-32.el8_10.x86_64.rpm
 libkadm5-1.18.2-33.el8_10.x86_64.rpm
 libkadm5-1.18.2-34.el8_10.i686.rpm
 libkadm5-1.18.2-34.el8_10.x86_64.rpm
 libldb-2.8.0-1.el8_10.x86_64.rpm
 libmount-2.32.1-48.el8_10.x86_64.rpm
 libndp-1.7-7.el8_10.x86_64.rpm
 libnfsidmap-2.3.3-68.el8_10.x86_64.rpm
 libnghttp2-1.33.0-6.el8_10.1.x86_64.rpm
 libnghttp2-1.33.0-6.el8_10.2.x86_64.rpm
 libnsl-2.28-251.el8_10.2.i686.rpm
 libnsl-2.28-251.el8_10.2.x86_64.rpm
 libnsl-2.28-251.el8_10.25.x86_64.rpm
 libnsl-2.28-251.el8_10.31.i686.rpm
 libnsl-2.28-251.el8_10.31.x86_64.rpm
 libnsl-2.28-251.el8_10.34.i686.rpm
 libnsl-2.28-251.el8_10.34.x86_64.rpm
 libnsl2-1.2.0-2.20180605git4a062cf.el8.x86_64.rpm
 libomp-17.0.6-1.module+el8.10.0+20808+e12784c0.x86_64.rpm
 libomp-devel-17.0.6-1.module+el8.10.0+20808+e12784c0.x86_64.rpm
 libpipeline-1.5.0-2.el8.x86_64.rpm

libpng-1.6.34-10.el8_10.x86_64.rpm
 libpq-13.23-1.el8_10.x86_64.rpm
 libpq-devel-13.23-1.el8_10.x86_64.rpm
 libproxy-0.4.15-5.5.el8_10.x86_64.rpm
 libselinux-2.9-10.el8_10.i686.rpm
 libselinux-2.9-10.el8_10.x86_64.rpm
 libselinux-2.9-11.el8_10.i686.rpm
 libselinux-2.9-11.el8_10.x86_64.rpm
 libselinux-devel-2.9-10.el8_10.x86_64.rpm
 libselinux-devel-2.9-11.el8_10.x86_64.rpm
 libselinux-utils-2.9-10.el8_10.x86_64.rpm
 libselinux-utils-2.9-11.el8_10.x86_64.rpm
 libsemanage-2.9-12.el8_10.x86_64.rpm
 libsemanage-2.9-9.el8_6.x86_64.rpm
 libsepol-2.9-3.el8.i686.rpm
 libsepol-devel-2.9-3.el8.i686.rpm
 libsepol-devel-2.9-3.el8.x86_64.rpm
 libslirp-4.4.0-2.module+el8.10.0+22931+799fd806.x86_64.rpm
 libslirp-4.4.0-2.module+el8.10.0+24081+a04d358a.x86_64.rpm
 libsmartcols-2.32.1-48.el8_10.x86_64.rpm
 libsoup-2.62.3-7.el8_10.x86_64.rpm
 libsoup-2.62.3-9.el8_10.x86_64.rpm
 libsoup-devel-2.62.3-9.el8_10.x86_64.rpm
 libss-1.45.6-5.el8.x86_64.rpm
 libss-1.45.6-7.el8_10.x86_64.rpm
 libssh-0.9.6-16.el8_10.x86_64.rpm
 libssh-config-0.9.6-16.el8_10.noarch.rpm
 libsss_autofs-2.9.4-3.el8_10.x86_64.rpm
 libsss_autofs-2.9.4-5.el8_10.4.x86_64.rpm
 libsss_certmap-2.9.4-3.el8_10.x86_64.rpm
 libsss_certmap-2.9.4-5.el8_10.4.x86_64.rpm
 libsss_idmap-2.9.4-3.el8_10.x86_64.rpm
 libsss_idmap-2.9.4-5.el8_10.4.x86_64.rpm
 libsss_nss_idmap-2.9.4-3.el8_10.x86_64.rpm
 libsss_nss_idmap-2.9.4-5.el8_10.4.x86_64.rpm
 libsss_sudo-2.9.4-3.el8_10.x86_64.rpm
 libsss_sudo-2.9.4-5.el8_10.4.x86_64.rpm
 libstdc++-8.5.0-26.el8_10.i686.rpm
 libstdc++-8.5.0-26.el8_10.x86_64.rpm
 libstdc++-8.5.0-28.el8_10.i686.rpm
 libstdc++-8.5.0-28.el8_10.x86_64.rpm
 libstdc++-devel-8.5.0-26.el8_10.x86_64.rpm
 libstdc++-devel-8.5.0-28.el8_10.x86_64.rpm

libtasn1-4.13-5.el8_10.i686.rpm
 libtasn1-4.13-5.el8_10.x86_64.rpm
 libtiff-4.0.9-33.el8_10.x86_64.rpm
 libtiff-4.0.9-34.el8_10.x86_64.rpm
 libtiff-4.0.9-36.el8_10.x86_64.rpm
 libtiff-4.0.9-37.el8_10.x86_64.rpm
 libtirpc-1.1.4-12.el8_10.x86_64.rpm
 libuser-0.62-26.el8_10.x86_64.rpm
 libuuid-2.32.1-48.el8_10.i686.rpm
 libuuid-2.32.1-48.el8_10.x86_64.rpm
 libuv-1.41.1-2.el8_10.x86_64.rpm
 libverto-devel-0.3.2-2.el8.x86_64.rpm
 libverto-libev-0.3.2-2.el8.x86_64.rpm
 libvirt-client-8.0.0-23.1.module+el8.10.0+21659+98b2ad6a.x86_64.rpm
 libvirt-daemon-8.0.0-23.1.module+el8.10.0+21659+98b2ad6a.x86_64.rpm
 libvirt-daemon-config-network-8.0.0-23.1.module+el8.10.0+21659+98b2ad6a.x86_64.rpm
 libvirt-daemon-driver-interface-8.0.0-23.1.module+el8.10.0+21659+98b2ad6a.x86_64.rpm
 libvirt-daemon-driver-network-8.0.0-23.1.module+el8.10.0+21659+98b2ad6a.x86_64.rpm
 libvirt-daemon-driver-nodedev-8.0.0-23.1.module+el8.10.0+21659+98b2ad6a.x86_64.rpm
 libvirt-daemon-driver-nwfilter-8.0.0-23.1.module+el8.10.0+21659+98b2ad6a.x86_64.rpm
 libvirt-daemon-driver-qemu-8.0.0-23.1.module+el8.10.0+21659+98b2ad6a.x86_64.rpm
 libvirt-daemon-driver-secret-8.0.0-23.1.module+el8.10.0+21659+98b2ad6a.x86_64.rpm
 libvirt-daemon-driver-storage-8.0.0-23.1.module+el8.10.0+21659+98b2ad6a.x86_64.rpm
 libvirt-daemon-driver-storage-core-8.0.0-23.1.module+el8.10.0+21659+98b2ad6a.x86_64.rpm
 libvirt-daemon-driver-storage-disk-8.0.0-23.1.module+el8.10.0+21659+98b2ad6a.x86_64.rpm
 libvirt-daemon-driver-storage-gluster-8.0.0-23.1.module+el8.10.0+21659+98b2ad6a.x86_64.rpm
 libvirt-daemon-driver-storage-iscsi-8.0.0-23.1.module+el8.10.0+21659+98b2ad6a.x86_64.rpm
 libvirt-daemon-driver-storage-iscsi-direct-8.0.0-23.1.module+el8.10.0+21659+98b2ad6a.x86_64.rpm
 libvirt-daemon-driver-storage-logical-8.0.0-23.1.module+el8.10.0+21659+98b2ad6a.x86_64.rpm
 libvirt-daemon-driver-storage-mpath-8.0.0-23.1.module+el8.10.0+21659+98b2ad6a.x86_64.rpm
 libvirt-daemon-driver-storage-rbd-8.0.0-23.1.module+el8.10.0+21659+98b2ad6a.x86_64.rpm
 libvirt-daemon-driver-storage-scsi-8.0.0-23.1.module+el8.10.0+21659+98b2ad6a.x86_64.rpm
 libvirt-daemon-kvm-8.0.0-23.1.module+el8.10.0+21659+98b2ad6a.x86_64.rpm
 libvirt-libs-8.0.0-23.1.module+el8.10.0+21659+98b2ad6a.x86_64.rpm
 libwebp-1.0.0-11.el8_10.x86_64.rpm
 libX11-1.6.8-9.el8_10.x86_64.rpm
 libX11-common-1.6.8-9.el8_10.noarch.rpm
 libxml2-2.9.7-19.el8_10.x86_64.rpm
 libxml2-2.9.7-21.el8_10.3.x86_64.rpm
 libxml2-2.9.7-21.el8_10.4.x86_64.rpm
 libxml2-devel-2.9.7-21.el8_10.3.x86_64.rpm
 libxml2-devel-2.9.7-21.el8_10.4.x86_64.rpm



libxslt-1.1.32-6.1.el8_10.x86_64.rpm
libxslt-1.1.32-6.3.el8_10.x86_64.rpm
libxslt-devel-1.1.32-6.3.el8_10.x86_64.rpm
linux-firmware-20260112-135.git486ac8f9.el8_10.noarch.rpm
linux-firmware-20260410-138.gitdc85cced.el8_10.noarch.rpm
liquibase-4.25.1-1.noarch.rpm
llvm-17.0.6-2.module+el8.10.0+21256+978ccea6.x86_64.rpm
llvm-devel-17.0.6-2.module+el8.10.0+21256+978ccea6.x86_64.rpm
llvm-googletest-17.0.6-2.module+el8.10.0+21256+978ccea6.x86_64.rpm
llvm-libs-17.0.6-2.module+el8.10.0+21256+978ccea6.x86_64.rpm
llvm-static-17.0.6-2.module+el8.10.0+21256+978ccea6.x86_64.rpm
llvm-test-17.0.6-2.module+el8.10.0+21256+978ccea6.x86_64.rpm
lshw-B.02.19.2-6.el8_10.1.x86_64.rpm
lvm2-2.03.14-15.el8_10.3.x86_64.rpm
lvm2-libs-2.03.14-15.el8_10.3.x86_64.rpm
lz4-1.8.3-3.el8_4.x86_64.rpm
lz4-libs-1.8.3-5.el8_10.i686.rpm
lz4-libs-1.8.3-5.el8_10.x86_64.rpm
man-db-2.7.6.1-18.el8.x86_64.rpm
mesa-libGL-23.1.4-3.el8_10.x86_64.rpm
mesa-libglapi-23.1.4-3.el8_10.x86_64.rpm
microcode_ctl-20251111-1.el8_10.x86_64.rpm
microcode_ctl-20260227-1.el8_10.x86_64.rpm
NetworkManager-1.40.16-15.el8_9.x86_64.rpm
NetworkManager-1.40.16-20.el8_10.x86_64.rpm
NetworkManager-adsl-1.40.16-15.el8_9.x86_64.rpm
NetworkManager-bluetooth-1.40.16-15.el8_9.x86_64.rpm
NetworkManager-config-server-1.40.16-15.el8_9.noarch.rpm
NetworkManager-libnm-1.40.16-15.el8_9.x86_64.rpm
NetworkManager-libnm-1.40.16-20.el8_10.x86_64.rpm
NetworkManager-team-1.40.16-15.el8_9.x86_64.rpm
NetworkManager-team-1.40.16-20.el8_10.x86_64.rpm
NetworkManager-tui-1.40.16-15.el8_9.x86_64.rpm
NetworkManager-tui-1.40.16-20.el8_10.x86_64.rpm
NetworkManager-wifi-1.40.16-15.el8_9.x86_64.rpm
NetworkManager-wwan-1.40.16-15.el8_9.x86_64.rpm
nftables-1.0.4-7.el8_10.x86_64.rpm
nodejs-22.13.1-1.module+el8.10.0+22759+46b58560.x86_64.rpm
nodejs-22.16.0-2.module+el8.10.0+23338+c5a38893.x86_64.rpm
nodejs-24.11.1-0.module+el8.10.0+23730+2ad7beb8.x86_64.rpm
nodejs-devel-22.16.0-2.module+el8.10.0+23338+c5a38893.x86_64.rpm
nodejs-docs-22.13.1-1.module+el8.10.0+22759+46b58560.noarch.rpm
nodejs-docs-22.16.0-2.module+el8.10.0+23338+c5a38893.noarch.rpm

nodejs-docs-24.11.1-0.module+el8.10.0+23730+2ad7beb8.noarch.rpm
 nodejs-full-i18n-22.13.1-1.module+el8.10.0+22759+46b58560.x86_64.rpm
 nodejs-full-i18n-22.16.0-2.module+el8.10.0+23338+c5a38893.x86_64.rpm
 nodejs-full-i18n-24.11.1-0.module+el8.10.0+23730+2ad7beb8.x86_64.rpm
 nodejs-libs-22.13.1-1.module+el8.10.0+22759+46b58560.x86_64.rpm
 nodejs-libs-22.16.0-2.module+el8.10.0+23338+c5a38893.x86_64.rpm
 nodejs-libs-24.11.1-0.module+el8.10.0+23730+2ad7beb8.x86_64.rpm
 nodejs-nodemod-3.0.1-1.module+el8.10.0+23140+4056b950.noarch.rpm
 nodejs-packaging-2021.06-4.module+el8.10.0+23140+4056b950.noarch.rpm
 nodejs-packaging-bundler-2021.06-4.module+el8.10.0+23140+4056b950.noarch.rpm
 npm-10.9.2-1.22.13.1.1.module+el8.10.0+22759+46b58560.x86_64.rpm
 npm-10.9.2-1.22.16.0.2.module+el8.10.0+23338+c5a38893.x86_64.rpm
 npm-11.6.2-1.24.11.1.0.module+el8.10.0+23730+2ad7beb8.noarch.rpm
 nspr-4.36.0-2.el8_10.x86_64.rpm
 nss-3.101.0-11.el8_8.x86_64.rpm
 nss-3.112.0-4.el8_10.x86_64.rpm
 nss-3.112.0-8.el8_10.x86_64.rpm
 nss-softokn-3.101.0-11.el8_8.x86_64.rpm
 nss-softokn-3.112.0-4.el8_10.x86_64.rpm
 nss-softokn-3.112.0-8.el8_10.x86_64.rpm
 nss-softokn-freebl-3.101.0-11.el8_8.x86_64.rpm
 nss-softokn-freebl-3.112.0-4.el8_10.x86_64.rpm
 nss-softokn-freebl-3.112.0-8.el8_10.x86_64.rpm
 nss-sysinit-3.101.0-11.el8_8.x86_64.rpm
 nss-sysinit-3.112.0-4.el8_10.x86_64.rpm
 nss-sysinit-3.112.0-8.el8_10.x86_64.rpm
 nss-tools-3.112.0-4.el8_10.x86_64.rpm
 nss-tools-3.112.0-8.el8_10.x86_64.rpm
 nss-util-3.101.0-11.el8_8.x86_64.rpm
 nss-util-3.112.0-4.el8_10.x86_64.rpm
 nss-util-3.112.0-8.el8_10.x86_64.rpm
 openldap-2.4.46-19.el8_10.x86_64.rpm
 openldap-2.4.46-21.el8_10.x86_64.rpm
 openresty-1.27.1.2-1.el8.x86_64.rpm
 openresty-openssl3-3.5.4-2.el8.x86_64.rpm
 openresty-pcre2-10.46-1.el8.x86_64.rpm
 openresty-zlib-1.3.1-1.el8.x86_64.rpm
 openssh-8.0p1-25.el8_10.x86_64.rpm
 openssh-8.0p1-27.el8_10.x86_64.rpm
 openssh-8.0p1-28.el8_10.x86_64.rpm
 openssh-8.0p1-29.el8_10.x86_64.rpm
 openssh-askpass-8.0p1-25.el8_10.x86_64.rpm
 openssh-clients-8.0p1-25.el8_10.x86_64.rpm

openssh-clients-8.0p1-27.el8_10.x86_64.rpm
 openssh-clients-8.0p1-28.el8_10.x86_64.rpm
 openssh-clients-8.0p1-29.el8_10.x86_64.rpm
 openssh-server-8.0p1-25.el8_10.x86_64.rpm
 openssh-server-8.0p1-27.el8_10.x86_64.rpm
 openssh-server-8.0p1-28.el8_10.x86_64.rpm
 openssh-server-8.0p1-29.el8_10.x86_64.rpm
 openssl-1.1.1k-14.el8_10.x86_64.rpm
 openssl-1.1.1k-14.el8_6.x86_64.rpm
 openssl-1.1.1k-15.el8_6.x86_64.rpm
 openssl-devel-1.1.1k-14.el8_10.x86_64.rpm
 openssl-devel-1.1.1k-14.el8_6.x86_64.rpm
 openssl-devel-1.1.1k-15.el8_6.x86_64.rpm
 openssl-devel-1.1.1k-9.el8_7.x86_64.rpm
 openssl-libs-1.1.1k-14.el8_10.i686.rpm
 openssl-libs-1.1.1k-14.el8_10.x86_64.rpm
 openssl-libs-1.1.1k-14.el8_6.i686.rpm
 openssl-libs-1.1.1k-14.el8_6.x86_64.rpm
 openssl-libs-1.1.1k-15.el8_6.i686.rpm
 openssl-libs-1.1.1k-15.el8_6.x86_64.rpm
 openssl-libs-1.1.1k-9.el8_7.i686.rpm
 orafce_17-4.14.4-1PGDG.rhel8.x86_64.rpm
 os-prober-1.74-11.el8_10.x86_64.rpm
 pam-1.3.1-36.el8_10.x86_64.rpm
 pam-1.3.1-37.el8_10.x86_64.rpm
 pam-1.3.1-39.el8_10.x86_64.rpm
 pbzip2-1.1.13-1.el8.x86_64.rpm
 pcre2-10.32-3.el8_6.i686.rpm
 pcre2-devel-10.32-3.el8_6.x86_64.rpm
 pcre2-utf16-10.32-3.el8_6.x86_64.rpm
 pcre2-utf32-10.32-3.el8_6.x86_64.rpm
 perl-5.26.3-423.el8_10.x86_64.rpm
 perl-Attribute-Handlers-0.99-423.el8_10.noarch.rpm
 perl-Config-IniFiles-2.83-1.x86_64.rpm
 perl-Convert-ASN1-0.27-1.x86_64.rpm
 perl-CPAN-2.18-402.el8_10.noarch.rpm
 perl-DBD-Oracle_19_0-1.80-1.x86_64.rpm
 perl-devel-5.26.3-423.el8_10.x86_64.rpm
 perl-Devel-Peek-1.26-423.el8_10.x86_64.rpm
 perl-Devel-SelfStubber-1.06-423.el8_10.noarch.rpm
 perl-Errno-1.28-423.el8_10.x86_64.rpm
 perl-Exporter-Tiny-1.002002-1.x86_64.rpm
 perl-ExtUtils-Embed-1.34-423.el8_10.noarch.rpm

perl-ExtUtils-Miniperl-1.06-423.el8_10.noarch.rpm
perl-Git-2.43.7-1.el8_10.noarch.rpm
perl-HTTP-Daemon-6.12-1.x86_64.rpm
perl-HTTP-Proxy-0.304-1.x86_64.rpm
perl-interpreter-5.26.3-423.el8_10.x86_64.rpm
perl-IO-1.38-423.el8_10.x86_64.rpm
perl-IO-Socket-INET6-2.72-1.x86_64.rpm
perl-IO-Socket-INET6-2.72-12.el8.noarch.rpm
perl-IO-Tty-1.12-11.el8.x86_64.rpm
perl-IO-Zlib-1.10-423.el8_10.noarch.rpm
perl-IPC-Run-0.99-1.el8.noarch.rpm
perl-ldap-0.68-1.x86_64.rpm
perl-libnetcfg-5.26.3-423.el8_10.noarch.rpm
perl-libs-5.26.3-423.el8_10.x86_64.rpm
perl-List-MoreUtils-0.430-1.x86_64.rpm
perl-Locale-Maketext-Simple-0.21-423.el8_10.noarch.rpm
perl-macros-5.26.3-423.el8_10.x86_64.rpm
perl-Math-Complex-1.59-423.el8_10.noarch.rpm
perl-Memoize-1.03-423.el8_10.noarch.rpm
perl-Module-Loaded-0.08-423.el8_10.noarch.rpm
perl-Net-Daemon-0.49-1.x86_64.rpm
perl-Net-IP-1.26-1.x86_64.rpm
perl-Net-IP-1.26-20.el8.noarch.rpm
perl-Net-Ping-2.55-423.el8_10.noarch.rpm
perl-Net-Telnet-3.04-1.x86_64.rpm
perl-open-1.11-423.el8_10.noarch.rpm
perl-PIRPC-0.2020-1.x86_64.rpm
perl-Pod-Html-1.22.02-423.el8_10.noarch.rpm
perl-Proc-ProcessTable-0.59-1.x86_64.rpm
perl-SelfLoader-1.23-423.el8_10.noarch.rpm
perl-Socket6-0.29-1.x86_64.rpm
perl-Test-1.30-423.el8_10.noarch.rpm
perl-Text-CSV-2.00-1.x86_64.rpm
perl-Text-Soundex-3.05-1.x86_64.rpm
perl-threads-2.21-2.el8.x86_64.rpm
perl-threads-shared-1.58-2.el8.x86_64.rpm
perl-Time-Piece-1.31-423.el8_10.x86_64.rpm
perl-Tk-FileDialog-1.3-1.x86_64.rpm
perl-utils-5.26.3-423.el8_10.noarch.rpm
perl-XML-Dumper-0.81-1.x86_64.rpm
perl-XML-Filter-BufferText-1.01-1.x86_64.rpm
perl-XML-LibXML-2.0132-2.el8.x86_64.rpm
perl-XML-Parser-2.44-12.el8_10.x86_64.rpm

perl-XML-RegExp-0.04-1.x86_64.rpm
 perl-XML-RegExp-0.04-14.el8.noarch.rpm
 perl-XML-SAX-Writer-0.57-1.x86_64.rpm
 pesign-0.112-27.el8_7.x86_64.rpm
 pgtt_17-4.4-1PGDG.rhel8.x86_64.rpm
 platform-python-3.6.8-69.el8_10.x86_64.rpm
 platform-python-3.6.8-71.el8_10.x86_64.rpm
 platform-python-3.6.8-73.el8_10.x86_64.rpm
 platform-python-3.6.8-74.el8_10.x86_64.rpm
 platform-python-3.6.8-75.el8_10.x86_64.rpm
 platform-python-3.6.8-76.el8_10.x86_64.rpm
 platform-python-setuptools-39.2.0-8.el8_10.noarch.rpm
 platform-python-setuptools-39.2.0-9.el8_10.noarch.rpm
 plymouth-0.9.4-12.20200615git1e36e30.el8_10.x86_64.rpm
 plymouth-core-libs-0.9.4-12.20200615git1e36e30.el8_10.x86_64.rpm
 plymouth-scripts-0.9.4-12.20200615git1e36e30.el8_10.x86_64.rpm
 podman-4.9.4-3.module+el8.10.0+21974+acd2159c.x86_64.rpm
 podman-catatonit-4.9.4-3.module+el8.10.0+21974+acd2159c.x86_64.rpm
 podman-gvproxy-4.9.4-3.module+el8.10.0+21974+acd2159c.x86_64.rpm
 podman-plugins-4.9.4-3.module+el8.10.0+21974+acd2159c.x86_64.rpm
 policycoreutils-2.9-26.el8_10.x86_64.rpm
 policycoreutils-python-utils-2.9-26.el8_10.noarch.rpm
 polkit-0.115-15.el8_10.2.x86_64.rpm
 polkit-libs-0.115-15.el8_10.2.x86_64.rpm
 postgresql-16.8-1.module+el8.10.0+22867+e4e13b1c.x86_64.rpm
 postgresql-private-devel-16.8-1.module+el8.10.0+22867+e4e13b1c.x86_64.rpm
 postgresql-private-libs-16.8-1.module+el8.10.0+22867+e4e13b1c.x86_64.rpm
 postgresql17-17.6-1PGDG.rhel8.x86_64.rpm
 postgresql17-contrib-17.6-1PGDG.rhel8.x86_64.rpm
 postgresql17-devel-17.6-1PGDG.rhel8.x86_64.rpm
 postgresql17-libs-17.6-1PGDG.rhel8.x86_64.rpm
 postgresql17-server-17.6-1PGDG.rhel8.x86_64.rpm
 postgresql_JDBC-42.6.2-1.el7.noarch.rpm
 python2-lxml-4.2.3-6.module+el8.9.0+19487+7dc18407.x86_64.rpm
 python3-audit-3.0.7-4.el8.x86_64.rpm
 python3-audit-3.1.2-1.el8_10.1.x86_64.rpm
 python3-bind-9.11.36-14.el8_10.noarch.rpm
 python3-bind-9.11.36-16.el8_10.2.noarch.rpm
 python3-cloud-what-1.28.44-1.el8_10.x86_64.rpm
 python3-dnf-4.7.0-21.el8_10.noarch.rpm
 python3-firewall-0.9.11-10.el8_10.noarch.rpm
 python3-hawkey-0.63.0-20.el8_10.x86_64.rpm
 python3-hawkey-0.63.0-21.el8_10.x86_64.rpm

python3-idna-2.5-7.el8_10.noarch.rpm
python3-leapp-0.19.0-1.el8_10.noarch.rpm
python3-libdnf-0.63.0-20.el8_10.x86_64.rpm
python3-libdnf-0.63.0-21.el8_10.x86_64.rpm
python3-libs-3.6.8-69.el8_10.x86_64.rpm
python3-libs-3.6.8-71.el8_10.x86_64.rpm
python3-libs-3.6.8-73.el8_10.x86_64.rpm
python3-libs-3.6.8-74.el8_10.x86_64.rpm
python3-libs-3.6.8-75.el8_10.x86_64.rpm
python3-libs-3.6.8-76.el8_10.x86_64.rpm
python3-libselinux-2.9-10.el8_10.x86_64.rpm
python3-libselinux-2.9-11.el8_10.x86_64.rpm
python3-libsemanage-2.9-12.el8_10.x86_64.rpm
python3-libsemanage-2.9-9.el8.x86_64.rpm
python3-libsemanage-2.9-9.el8_6.x86_64.rpm
python3-libxml2-2.9.7-19.el8_10.x86_64.rpm
python3-libxml2-2.9.7-21.el8_10.3.x86_64.rpm
python3-libxml2-2.9.7-21.el8_10.4.x86_64.rpm
python3-lxml-4.2.3-4.el8.x86_64.rpm
python3-lxml-4.2.5-2.el8ost.x86_64.rpm
python3-magic-5.33-27.el8_10.noarch.rpm
python3-nftables-1.0.4-7.el8_10.x86_64.rpm
python3-perf-4.18.0-553.104.1.el8_10.x86_64.rpm
python3-perf-4.18.0-553.111.1.el8_10.x86_64.rpm
python3-perf-4.18.0-553.117.1.el8_10.x86_64.rpm
python3-perf-4.18.0-553.123.1.el8_10.x86_64.rpm
python3-perf-4.18.0-553.124.1.el8_10.x86_64.rpm
python3-perf-4.18.0-553.50.1.el8_10.x86_64.rpm
python3-policycoreutils-2.9-26.el8_10.noarch.rpm
python3-requests-2.20.0-6.el8_10.noarch.rpm
python3-rpm-4.14.3-32.el8_10.x86_64.rpm
python3-setools-4.3.0-3.el8.x86_64.rpm
python3-setuptools-39.2.0-8.el8_10.noarch.rpm
python3-setuptools-39.2.0-9.el8_10.noarch.rpm
python3-setuptools-wheel-39.2.0-8.el8_10.noarch.rpm
python3-setuptools-wheel-39.2.0-9.el8_10.noarch.rpm
python3-sssdconfig-2.9.4-3.el8_10.noarch.rpm
python3-sssdconfig-2.9.4-4.el8_10.noarch.rpm
python3-subscription-manager-rhsm-1.28.44-1.el8_10.x86_64.rpm
python3-syspurpose-1.28.44-1.el8_10.x86_64.rpm
python3-unbound-1.16.2-5.8.el8_10.x86_64.rpm
python3-unbound-1.16.2-5.9.el8_10.x86_64.rpm
python3-urllib3-1.24.2-8.el8_10.noarch.rpm

python3-urllib3-1.24.2-9.el8_10.noarch.rpm
python3.11-3.11.11-1.el8_10.x86_64.rpm
python3.11-3.11.13-1.el8_10.x86_64.rpm
python3.11-3.11.13-5.el8_10.x86_64.rpm
python3.11-3.11.13-7.el8_10.x86_64.rpm
python3.11-cffi-1.15.1-1.el8.x86_64.rpm
python3.11-charset-normalizer-2.1.0-1.el8.noarch.rpm
python3.11-cryptography-37.0.2-6.el8.x86_64.rpm
python3.11-devel-3.11.11-1.el8_10.x86_64.rpm
python3.11-devel-3.11.13-1.el8_10.x86_64.rpm
python3.11-devel-3.11.13-5.el8_10.x86_64.rpm
python3.11-devel-3.11.13-7.el8_10.x86_64.rpm
python3.11-idna-3.4-1.el8.noarch.rpm
python3.11-libs-3.11.11-1.el8_10.x86_64.rpm
python3.11-libs-3.11.13-1.el8_10.x86_64.rpm
python3.11-libs-3.11.13-5.el8_10.x86_64.rpm
python3.11-libs-3.11.13-7.el8_10.x86_64.rpm
python3.11-lxml-4.9.2-4.el8.x86_64.rpm
python3.11-mod_wsgi-4.9.4-1.el8.x86_64.rpm
python3.11-numpy-1.23.5-1.el8.x86_64.rpm
python3.11-numpy-f2py-1.23.5-1.el8.x86_64.rpm
python3.11-pip-22.3.1-5.el8.noarch.rpm
python3.11-pip-wheel-22.3.1-5.el8.noarch.rpm
python3.11-ply-3.11-1.el8.noarch.rpm
python3.11-psycopg2-2.9.3-1.el8.x86_64.rpm
python3.11-pycparser-2.20-1.el8.noarch.rpm
python3.11-PyMySQL-1.0.2-2.el8_10.noarch.rpm
python3.11-pysocks-1.7.1-1.el8.noarch.rpm
python3.11-pyyaml-6.0-1.el8.x86_64.rpm
python3.11-requests-2.28.1-1.el8.noarch.rpm
python3.11-rpm-macros-3.11.13-1.el8_10.noarch.rpm
python3.11-scipy-1.10.1-2.el8.x86_64.rpm
python3.11-setuptools-65.5.1-3.el8_10.noarch.rpm
python3.11-setuptools-65.5.1-4.el8_10.noarch.rpm
python3.11-setuptools-wheel-65.5.1-3.el8_10.noarch.rpm
python3.11-setuptools-wheel-65.5.1-4.el8_10.noarch.rpm
python3.11-six-1.16.0-1.el8.noarch.rpm
python3.11-tkinter-3.11.13-1.el8_10.x86_64.rpm
python3.11-urllib3-1.26.12-5.el8_10.noarch.rpm
python3.11-wheel-0.38.4-4.el8.noarch.rpm
python3.12-3.12.11-2.el8_10.x86_64.rpm
python3.12-3.12.12-2.el8_10.x86_64.rpm
python3.12-3.12.12-3.el8_10.x86_64.rpm

python3.12-3.12.12-4.el8_10.x86_64.rpm
python3.12-3.12.13-2.el8_10.x86_64.rpm
python3.12-3.12.8-1.el8_10.x86_64.rpm
python3.12-devel-3.12.11-2.el8_10.x86_64.rpm
python3.12-devel-3.12.12-2.el8_10.x86_64.rpm
python3.12-devel-3.12.12-3.el8_10.x86_64.rpm
python3.12-devel-3.12.13-2.el8_10.x86_64.rpm
python3.12-devel-3.12.8-1.el8_10.i686.rpm
python3.12-devel-3.12.8-1.el8_10.x86_64.rpm
python3.12-libs-3.12.11-2.el8_10.x86_64.rpm
python3.12-libs-3.12.12-2.el8_10.x86_64.rpm
python3.12-libs-3.12.12-3.el8_10.x86_64.rpm
python3.12-libs-3.12.12-4.el8_10.x86_64.rpm
python3.12-libs-3.12.13-2.el8_10.x86_64.rpm
python3.12-libs-3.12.8-1.el8_10.i686.rpm
python3.12-libs-3.12.8-1.el8_10.x86_64.rpm
python3.12-lxml-4.9.3-2.el8.x86_64.rpm
python3.12-rpm-macros-3.12.8-1.el8_10.noarch.rpm
python3.12-setuptools-68.2.2-4.el8_10.noarch.rpm
python3.12-setuptools-68.2.2-5.el8_10.noarch.rpm
python3.12-setuptools-wheel-68.2.2-4.el8_10.noarch.rpm
python3.12-tkinter-3.12.8-1.el8_10.x86_64.rpm
python38-lxml-4.4.1-7.module+el8.9.0+19598+4a60c7b7.x86_64.rpm
python39-lxml-4.6.5-1.module+el8.9.0+19644+d68f775d.x86_64.rpm
qemu-guest-agent-6.2.0-53.module+el8.10.0+23760+c0926e61.6.x86_64.rpm
redhat-release-8.10-0.3.el8.x86_64.rpm
redhat-release-eula-8.10-0.3.el8.x86_64.rpm
rhc-0.2.5-4.el8_10.x86_64.rpm
rhc-0.2.5-5.el8_10.x86_64.rpm
rhc-0.2.5-6.el8_10.x86_64.rpm
rhc-0.2.5-7.el8_10.x86_64.rpm
rng-tools-6.16-2.el8_10.x86_64.rpm
rpm-4.14.3-32.el8_10.x86_64.rpm
rpm-build-4.14.3-32.el8_10.x86_64.rpm
rpm-build-libs-4.14.3-32.el8_10.x86_64.rpm
rpm-libs-4.14.3-32.el8_10.x86_64.rpm
rpm-plugin-selinux-4.14.3-32.el8_10.x86_64.rpm
rpm-plugin-systemd-inhibit-4.14.3-32.el8_10.x86_64.rpm
rpm-sign-4.14.3-32.el8_10.x86_64.rpm
rsync-3.1.3-20.el8_10.x86_64.rpm
rsync-3.1.3-23.el8_10.x86_64.rpm
rsync-3.1.3-24.el8_10.x86_64.rpm
rsync-3.1.3-25.el8_10.x86_64.rpm

rsyslog-8.2102.0-15.el8_10.1.x86_64.rpm
rsyslog-gnutls-8.2102.0-15.el8_10.1.x86_64.rpm
rsyslog-relp-8.2102.0-15.el8_10.1.x86_64.rpm
runc-1.1.12-1.module+el8.10.0+21974+acd2159c.x86_64.rpm
scl-utils-2.0.2-16.el8.x86_64.rpm
sed-4.5-5.el8_10.x86_64.rpm
selinux-policy-3.14.3-139.el8_10.2.noarch.rpm
selinux-policy-targeted-3.14.3-139.el8_10.2.noarch.rpm
shadow-utils-4.6-23.el8_10.x86_64.rpm
slirp4netns-1.2.3-1.module+el8.10.0+22931+799fd806.x86_64.rpm
slirp4netns-1.2.3-1.module+el8.10.0+24081+a04d358a.x86_64.rpm
socat-1.7.4.1-2.el8_10.x86_64.rpm
sos-4.7.1-2.el8_10.noarch.rpm
source-highlight-3.1.8-18.el8_10.x86_64.rpm
sqlite-libs-3.26.0-20.el8_10.x86_64.rpm
sssd-2.9.4-3.el8_10.x86_64.rpm
sssd-ad-2.9.4-3.el8_10.x86_64.rpm
sssd-client-2.9.4-3.el8_10.x86_64.rpm
sssd-client-2.9.4-5.el8_10.4.x86_64.rpm
sssd-common-2.9.4-3.el8_10.x86_64.rpm
sssd-common-2.9.4-5.el8_10.4.x86_64.rpm
sssd-common-pac-2.9.4-3.el8_10.x86_64.rpm
sssd-ipa-2.9.4-3.el8_10.x86_64.rpm
sssd-kcm-2.9.4-3.el8_10.x86_64.rpm
sssd-kcm-2.9.4-5.el8_10.4.x86_64.rpm
sssd-krb5-2.9.4-3.el8_10.x86_64.rpm
sssd-krb5-common-2.9.4-3.el8_10.x86_64.rpm
sssd-ldap-2.9.4-3.el8_10.x86_64.rpm
sssd-nfs-idmap-2.9.4-3.el8_10.x86_64.rpm
sssd-nfs-idmap-2.9.4-5.el8_10.4.x86_64.rpm
sssd-proxy-2.9.4-3.el8_10.x86_64.rpm
strace-5.18-2.1.el8_10.x86_64.rpm
subscription-manager-1.28.44-1.el8_10.x86_64.rpm
sudo-1.9.5p2-1.el8_10.1.x86_64.rpm
sudo-1.9.5p2-1.el8_10.3.x86_64.rpm
sudo-1.9.5p2-1.el8_10.5.x86_64.rpm
sushi-3.28.3-3.el8_10.x86_64.rpm
sysstat-11.7.3-13.el8_10.x86_64.rpm
systemd-239-82.el8_10.1.x86_64.rpm
systemd-239-82.el8_10.13.x86_64.rpm
systemd-239-82.el8_10.15.x86_64.rpm
systemd-239-82.el8_10.16.x86_64.rpm
systemd-container-239-82.el8_10.1.x86_64.rpm

systemd-libs-239-82.el8_10.1.x86_64.rpm
 systemd-libs-239-82.el8_10.13.x86_64.rpm
 systemd-libs-239-82.el8_10.15.x86_64.rpm
 systemd-libs-239-82.el8_10.16.x86_64.rpm
 systemd-pam-239-82.el8_10.1.x86_64.rpm
 systemd-pam-239-82.el8_10.13.x86_64.rpm
 systemd-pam-239-82.el8_10.15.x86_64.rpm
 systemd-pam-239-82.el8_10.16.x86_64.rpm
 systemd-udev-239-82.el8_10.1.x86_64.rpm
 systemd-udev-239-82.el8_10.13.x86_64.rpm
 systemd-udev-239-82.el8_10.15.x86_64.rpm
 systemd-udev-239-82.el8_10.16.x86_64.rpm
 TAO_PNS-1.4l_p9-5.x86_64.rpm
 TAO_PNS-libs-1.4l_p9-5.i386.rpm
 TAO_PNS-libs-1.4l_p9-5.x86_64.rpm
 tar-1.30-11.el8_10.x86_64.rpm
 tbb-2018.2-10.el8_10.1.x86_64.rpm
 tcp_wrappers-libs-7.6-96.el8.x86_64.rpm
 tigervnc-license-1.13.1-10.el8_10.noarch.rpm
 tigervnc-server-minimal-1.13.1-10.el8_10.x86_64.rpm
 tomcat-9.0.87-1.el8_10.2.noarch.rpm
 tomcat-admin-webapps-9.0.87-1.el8_10.2.noarch.rpm
 tomcat-docs-webapp-9.0.87-1.el8_10.2.noarch.rpm
 tomcat-el-3.0-api-9.0.87-1.el8_10.2.noarch.rpm
 tomcat-jsp-2.3-api-9.0.87-1.el8_10.2.noarch.rpm
 tomcat-lib-9.0.87-1.el8_10.2.noarch.rpm
 tomcat-servlet-4.0-api-9.0.87-1.el8_10.2.noarch.rpm
 tomcat-webapps-9.0.87-1.el8_10.2.noarch.rpm
 tuned-2.22.1-4.el8_10.1.noarch.rpm
 tuned-2.22.1-6.el8_10.noarch.rpm
 tzdata-2025b-1.el8.noarch.rpm
 tzdata-2025c-1.el8.noarch.rpm
 tzdata-2026a-1.el8.noarch.rpm
 tzdata-java-2025b-1.el8.noarch.rpm
 tzdata-java-2026a-1.el8.noarch.rpm
 unbound-libs-1.16.2-5.8.el8_10.x86_64.rpm
 unbound-libs-1.16.2-5.9.el8_10.x86_64.rpm
 unzip-6.0-48.el8_10.x86_64.rpm
 upower-0.99.7-4.el8_7.x86_64.rpm
 util-linux-2.32.1-48.el8_10.x86_64.rpm
 valgrind-3.22.0-3.el8_10.i686.rpm
 valgrind-3.22.0-3.el8_10.x86_64.rpm
 valgrind-devel-3.22.0-3.el8_10.i686.rpm

valgrind-devel-3.22.0-3.el8_10.x86_64.rpm
 valgrind-docs-3.22.0-3.el8_10.x86_64.rpm
 valgrind-gdb-3.22.0-3.el8_10.x86_64.rpm
 valgrind-scripts-3.22.0-3.el8_10.x86_64.rpm
 valkey-8.0.6-1.el8.x86_64.rpm
 vdo-6.2.11.5-14.el8_10.x86_64.rpm
 vim-common-8.0.1763-22.el8_10.3.x86_64.rpm
 vim-common-8.0.1763-22.el8_10.x86_64.rpm
 vim-enhanced-8.0.1763-22.el8_10.3.x86_64.rpm
 vim-enhanced-8.0.1763-22.el8_10.x86_64.rpm
 vim-filesystem-8.0.1763-22.el8_10.3.noarch.rpm
 vim-filesystem-8.0.1763-22.el8_10.noarch.rpm
 vim-minimal-8.0.1763-22.el8_10.1.x86_64.rpm
 vim-minimal-8.0.1763-22.el8_10.3.x86_64.rpm
 vim-minimal-8.0.1763-22.el8_10.x86_64.rpm
 wget-1.19.5-12.el8_10.x86_64.rpm
 which-2.21-21.el8_10.x86_64.rpm
 words-3.0-28.el8.noarch.rpm
 xalan-j2-2.7.1-38.module+el8+2468+c564cec5.noarch.rpm
 xalan-j2-2.7.2-2.module_el8.7.0+3542+f1ef105f.noarch.rpm
 xerces-c-3.2.5-1.el8.x86_64.rpm
 xerces-j2-2.11.0-34.module+el8.10.0+20993+d0f024b0.noarch.rpm
 xerces-j2-2.12.0-4.module_el8.7.0+3542+f1ef105f.noarch.rpm
 xfsdump-3.1.8-7.el8_9.x86_64.rpm
 xml-commons-resolver-1.2-26.module+el8.10.0+20993+d0f024b0.noarch.rpm
 xorg-x11-server-common-1.20.11-25.el8_10.x86_64.rpm
 xorg-x11-server-Xorg-1.20.11-25.el8_10.x86_64.rpm
 xorg-x11-server-Xvfb-1.20.11-25.el8_10.x86_64.rpm
 xorg-x11-server-Xwayland-21.1.3-16.el8_10.x86_64.rpm
 yum-4.7.0-21.el8_10.noarch.rpm
 zlib-1.2.11-25.el8.i686.rpm
 Oracle19c_RDBMS-server-19.0.0.0-2604DBRU.1.tar.gz

3.2.3 Oracle client Updates on Containers

- Oracle19c_RDBMS-client-19.0.0.0-2604DBRUu.1.el7.x86_64
- Oracle19c_RDBMS-19.0.0.0-2604DBRUu.1.el7.x86_64
- Oracle19c_JDBC-19.0.0.0-2604DBRUu.1.el7.x86_64

4 Installation

Pre-Installation Steps:

Prerequisite: WSNOC-25.12.0-6880260402-FP1 Load already installed on the bench.

Installation steps:

1. Download packages to DEPOT of WSNOC-25.12.0-6880260402-FP1 load replacing the older ws-os,mnc-plat,mnc-oracle and wsnoc-sw iso.
2. Follow the Installation Guide for further installation steps.