



CVE-2023-48795

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2023-48795
State	PUBLISHED
Assigner	Unknown
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-12-18 16:15:00 UTC
Updated	2024-03-13 21:15:00 UTC
Description	Description unavailable.

Risk And Classification

Problem Types: CWE-354

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Sshd	All	All	All	All
Application	Apache	Sshj	All	All	All	All
Operating System	Apple	Macos	-	All	All	All
Application	Asynccssh Project	Asynccssh	All	All	All	All
Application	Bitvise	Ssh Client	All	All	All	All
Application	Bitvise	Ssh Server	All	All	All	All
Application	Connectbot	Sshlib	All	All	All	All
Application	Crates	Thrussh	All	All	All	All
Application	Crushftp	Crushftp	All	All	All	All
Application	Crushftp	Crushftp	All	All	All	All
Operating System	Debian	Debian Linux	-	All	All	All
Application	Dropbear Ssh Project	Dropbear Ssh	All	All	All	All
Application	Erlang	Erlang/otp	All	All	All	All
Application	Filezilla-project	Filezilla Client	All	All	All	All
Operating System	Freebsd	Freebsd	All	All	All	All
Application	Gentoo	Security	-	All	All	All
Application	Golang	Crypto	All	All	All	All

Application	Jadaptive	Maverick Synergy Java Ssh Api	All	All	All	All
Application	Kitty Project	Kitty	All	All	All	All
Operating System	Lancom-systems	Lanconfig	-	All	All	All
Operating System	Lancom-systems	Lcos	All	All	All	All
Operating System	Lancom-systems	Lcos Fx	-	All	All	All
Operating System	Lancom-systems	Lcos Lx	-	All	All	All
Operating System	Lancom-systems	Lcos Sx	4.20	All	All	All
Operating System	Lancom-systems	Lcos Sx	5.20	All	All	All
Application	Libssh	Libssh	All	All	All	All
Application	Libssh2	Libssh2	All	All	All	All
Application	Matez	Jsch	All	All	All	All
Application	Microsoft	Powershell	All	All	All	All
Application	Net-ssh	Net-ssh	7.2.0	All	All	All
Application	Netgate	Pfsense Ce	All	All	All	All
Application	Netgate	Pfsense Plus	All	All	All	All
Application	Netsarang	Xshell 7	All	All	All	All
Application	Openbsd	Openssh	All	All	All	All
Application	Oryx-embedded	Cyclone Ssh	All	All	All	All
Application	Panic	Nova	All	All	All	All
Application	Panic	Transmit 5	All	All	All	All
Application	Paramiko	Paramiko	All	All	All	All
Application	Proftpd	Proftpd	All	All	All	All
Application	Putty	Putty	All	All	All	All
Application	Redhat	Advanced Cluster Security	3.0	All	All	All
Application	Redhat	Advanced Cluster Security	4.0	All	All	All
Application	Redhat	Ceph Storage	6.0	All	All	All
Application	Redhat	Cert-manager Operator For Red Hat Openshift	-	All	All	All
Application	Redhat	Discovery	-	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Operating System	Redhat	Enterprise Linux	9.0	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	7.0	All	All	All
Application	Redhat	Keycloak	-	All	All	All
Application	Redhat	Openshift Api For Data Protection	-	All	All	All
Application	Redhat	Openshift Container Platform	4.0	All	All	All
Application	Redhat	Openshift Data Foundation	4.0	All	All	All
Application	Redhat	Openshift Developer Tools And Services	All	All	All	All

Application	Redhat	Openshift Developer Tools And Services	-	All	All	All
Application	Redhat	Openshift Dev Spaces	-	All	All	All
Application	Redhat	Openshift Gitops	-	All	All	All
Application	Redhat	Openshift Pipelines	-	All	All	All
Application	Redhat	Openshift Serverless	-	All	All	All
Application	Redhat	Openshift Virtualization	4	All	All	All
Application	Redhat	Openstack Platform	16.1	All	All	All
Application	Redhat	Openstack Platform	16.2	All	All	All
Application	Redhat	Openstack Platform	17.1	All	All	All
Application	Redhat	Single Sign-on	7.0	All	All	All
Application	Redhat	Storage	3.0	All	All	All
Application	Roumenpetrov	Pkixssh	All	All	All	All
Application	Russh Project	Russh	All	All	All	All
Application	Sftpgo Project	Sftpgo	All	All	All	All
Application	Ssh	Ssh	All	All	All	All
Application	Ssh2 Project	Ssh2	All	All	All	All
Application	Tera Term Project	Tera Term	All	All	All	All
Operating System	Thorntech	Sftp Gateway Firmware	All	All	All	All
Application	Tinyssh	Tinyssh	All	All	All	All
Application	Trilead	Ssh2	6401	All	All	All
Application	Vandyke	Securecr	All	All	All	All
Application	Winscp	Winscp	All	All	All	All

References

Reference	Source	Link
Security Advisory		psirt.g
github.com/mwiede/jsch/issues/457		github.
[SECURITY] Fedora 39 Update: putty-0.80-1.fc39 - package-announce - Fedora Mailing-Lists		lists.fe
bugzilla.suse.com/show_bug.cgi		bugzill
github.com/erlang/otp/blob/d1b43dc0f1361d2ad67601169e90a7fc50bb0369/lib/...		github.
[SECURITY] Fedora 38 Update: golang-x-mod-0.14.0-1.fc38 - package-announce - Fedora Mailing-Lists		lists.fe
news.ycombinator.com/item		news.y
www.reddit.com/r/sysadmin/comments/18idv52/cve202348795_why_is_this_cve_stil...		www.re
www.terrapin-attack.com		www.te
github.com/libssh2/libssh2/pull/1291		github.
github.com/ronf/asyncssh/tags		github.

github.com/paramiko/paramiko/issues/2337	github.
FEDORA-2023-20feb865d8	lists.fe
jadaptive.com/important-java-ssh-security-update-new-ssh-vulnerability-disc...	jadapti
github.com/rapier1/hpn-ssh/releases	github.
oryx-embedded.com/download	oryx-er
www.chiark.greenend.org.uk/~sgtatham/putty/changes.html	www.c
forum.netgate.com/topic/184941/terrapin-ssh-attack	forum.i
github.com/cyd01/KiTTY/issues/520	github.
github.com/advisories/GHSA-45x7-px36-x8w8	github.
[SECURITY] Fedora 38 Update: libssh-0.10.6-2.fc38 - package-announce - Fedora Mailing-Lists	lists.fe
FEDORA-2023-e77300e4b5	lists.fe
FEDORA-2023-0733306be9	lists.fe
help.panic.com/releasenotes/transmit5	help.pa
FEDORA-2023-cb8c606fbb	lists.fe
github.com/net-ssh/net-ssh/blob/2e65064a52d73396bfc3806c9196fc8108f33cd8...	github.
github.com/proftpd/proftpd/blob/d21e7a2e47e9b38f709bec58e3fa711f759ad0e1...	github.
support.apple.com/kb/HT214084	suppor
github.com/proftpd/proftpd/issues/456	github.
access.redhat.com/security/cve/cve-2023-48795	access
github.com/apache/mina-sshd/issues/445	github.
github.com/hierynomus/sshj/issues/916	github.
security-tracker.debian.org/tracker/source-package/proftpd-dfsg	securit
github.com/janmojis/tinyssh/issues/81	github.
[SECURITY] Fedora 39 Update: prometheus-podman-exporter-1.7.0-1.fc39 - package-announce - Fedora Mailing-Lists	lists.fe
github.com/PowerShell/Win32-OpenSSH/releases/tag/v9.5.0.0p1-Beta	github.
github.com/drakkan/sftpgo/releases/tag/v2.5.6	github.
matt.ucc.asn.au/dropbear/CHANGES	matt.uc
[oss-security] 20231218 CVE-2023-48795: Prefix Truncation Attacks in SSH Specification (Terrapin Attack)	www.o
github.com/connectbot/sshlib/commit/5c8b534f6e97db7ac0e0e579331213aa25c1...	github.
github.com/mkj/dropbear/blob/17657c36cce6df7716d5ff151ec09a665382d5dd/CH...	github.
www.theregister.com/2023/12/20/terrapin_attack_ssh	www.th
bugs.gentoo.org/920280	bugs.g
crates.io/crates/thrussh/versions	crates.
[SECURITY] [DLA 3719-1] phpseclib security update	lists.de
www.paramiko.org/changelog.html	www.p
security.netapp.com/advisory/ntan-20240105-0004	securit

security.metapp.com/advisory/map-2023-10-0007	secu...
FEDORA-2023-153404713b	lists.fe
github.com/proftpd/proftpd/blob/master/RELEASE_NOTES	github.
github.com/TeraTermProject/teraterm/commit/7279fd6ef4d0c8bdd6a90af4ada2...	github.
github.com/jtستا/ssh-audit/commit/8e972c5e94b460379fe0c7d20209c16df81538a5	github.
github.com/golang/crypto/commit/9d2ee975ef9fe627bf0a6f01c1f69e8ef1d4f05d	github.
news.ycombinator.com/item	news.y
www.openwall.com/lists/oss-security/2023/12/18/2	www.o
www.openssh.com/txt/release-9.6	www.o
[SECURITY] Fedora 38 Update: podman-4.8.3-1.fc38 - package-announce - Fedora Mailing-Lists	lists.fe
twitter.com/TrueSkrillor/status/1736774389725565005	twitter.
www.suse.com/c/suse-addresses-the-ssh-v2-protocol-terrapin-attack-aka-cve-...	www.s
security-tracker.debian.org/tracker/source-package/trilead-ssh2	securit
www.crushftp.com/crush10wiki/Wiki.jsp	www.c
github.com/openssh/openssh-portable/commits/master	github.
nova.app/releases	nova.a
GLSA-202312-17	securit
[SECURITY] Fedora 39 Update: podman-4.8.3-1.fc39 - package-announce - Fedora Mailing-Lists	lists.fe
security-tracker.debian.org/tracker/CVE-2023-48795	securit
thorntech.com/cve-2023-48795-and-sftp-gateway	thornte
news.ycombinator.com/item	news.y
[SECURITY] Fedora 39 Update: golang-x-mod-0.14.0-1.fc39 - package-announce - Fedora Mailing-Lists	lists.fe
ubuntu.com/security/CVE-2023-48795	ubuntu
github.com/proftpd/proftpd/blob/0a7ea9b0ba9fcdf368374a226370d08f10397d99...	github.
[SECURITY] Fedora 39 Update: golang-x-crypto-0.18.0-1.fc39 - package-announce - Fedora Mailing-Lists	lists.fe
www.bitvise.com/ssh-server-version-history	www.b
FEDORA-2023-b87ec6cf47	lists.fe
bugzilla.redhat.com/show_bug.cgi	bugzill
Debian -- Security Information -- DSA-5588-1 putty	www.d
[SECURITY] [DLA 3694-1] openssh security update	lists.de
git.libssh.org/projects/libssh.git/commit	git.lib:
winscp.net/eng/docs/history	winscp
github.com/mscdex/ssh2/commit/97b223f8891b96d6fc054df5ab1d5a1a545da2a3	github.
arstechnica.com/security/2023/12/hackers-can-break-ssh-channel-integrity-usin...	arstec
github.com/NixOS/nixpkgs/pull/275249	github.
github.com/PowerShell/Win32-OpenSSH/issues/2189	github.

[SECURITY] Fedora 38 Update: prometheus-podman-exporter-1.7.0-1.fc38 - package-announce - Fedora Mailing-Lists	lists.fe
nest.pijul.com/pijul/thrussh/changes/D6H7OWTTMHX6BTB3B6MNB0BX2L66CBL4LGSEUS...	nest.pi
github.com/ronf/asynssh/blob/develop/docs/changes.rst	github.
[SECURITY] Fedora 38 Update: golang-x-crypto-0.18.0-1.fc38 - package-announce - Fedora Mailing-Lists	lists.fe
Debian -- Security Information -- DSA-5586-1 openssh	www.d
gitlab.com/libssh/libssh-mirror/-/tags	gitlab.c
github.com/mwiede/jsch/pull/461	github.
filezilla-project.org/versions.php	filezilla
github.com/mwiede/jsch/compare/jsch-0.2.14...jsch-0.2.15	github.
www.netsarang.com/en/xshell-update-history	www.n
www.openssh.com/openbsd.html	www.o
github.com/connectbot/sshlib/compare/2.2.21...2.2.22	github.
[oss-security] 20231219 Re: CVE-2023-48795: Prefix Truncation Attacks in SSH Specification (Terrapin Attack)	www.o
www.freebsd.org/security/advisories/FreeBSD-SA-23:19.openssh.asc	www.fr
www.bitvise.com/ssh-client-version-history	www.b
github.com/erlang/otp/releases/tag/OTP-26.2.1	github.
packetstormsecurity.com/files/176280/Terrapin-SSH-Connection-Weakening.html	packet
www.openwall.com/lists/oss-security/2023/12/20/3	www.o
20240313 APPLE-SA-03-07-2024-2 macOS Sonoma 14.4	seclis
[SECURITY] Fedora 38 Update: python-paramiko-3.4.0-1.fc38 - package-announce - Fedora Mailing-Lists	lists.fe
github.com/ssh-mitm/ssh-mitm/issues/165	github.
[SECURITY] [DLA 3718-1] php-phpseclib security update	lists.de
[oss-security] 20231220 Re: CVE-2023-48795: Prefix Truncation Attacks in SSH Specification (Terrapin Attack)	www.o
roumenpetrov.info/secsh	roume
www.vandyke.com/products/securecrt/history.txt	www.v
groups.google.com/g/golang-announce/c/-n5WqVC18LQ	groups
www.lancom-systems.de/service-support/allgemeine-sicherheitshinweise	www.la
GLSA-202312-16	securit
github.com/TeraTermProject/teraterm/releases/tag/v5.1	github.
security-tracker.debian.org/tracker/source-package/libssh2	securit
groups.google.com/g/golang-announce/c/qA3XtxvMUyg	groups
github.com/warp-tech/russh/releases/tag/v0.40.2	github.
[SECURITY] Fedora 38 Update: putty-0.80-1.fc38 - package-announce - Fedora Mailing-Lists	lists.fe
CVE Program record	CVE.ORG www.c
NVD vulnerability detail	NVD nvd.nis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

161329 Oracle Enterprise Linux Security Update for libssh (ELSA-2024-0628)
161330 Oracle Enterprise Linux Security Update for openssh (ELSA-2024-0606)
161350 Oracle Enterprise Linux Security Update for openssh (ELSA-2024-12158)
161351 Oracle Enterprise Linux Security Update for openssh (ELSA-2024-12157)
161357 Oracle Enterprise Linux Security Update for openssh (ELSA-2024-12164)
161396 Oracle Enterprise Linux Security Update for openssh (ELSA-2024-1130)
161405 Oracle Enterprise Linux Security Update for buildah (ELSA-2024-1150)
161419 Oracle Enterprise Linux Security Update for openssh (ELSA-2024-12233)
161420 Oracle Enterprise Linux Security Update for openssh (ELSA-2024-12232)
200017 Ubuntu Security Notification for libssh Vulnerability (USN-6561-1)
200018 Ubuntu Security Notification for OpenSSH Vulnerabilities (USN-6560-1)
200041 Ubuntu Security Notification for OpenSSH Vulnerabilities (USN-6560-2)
200046 Ubuntu Security Notification for libssh2 Vulnerability (USN-6585-1)
200057 Ubuntu Security Notification for FileZilla Vulnerability (USN-6589-1)
200069 Ubuntu Security Notification for Paramiko Vulnerability (USN-6598-1)
242764 Red Hat Update for libssh (RHSA-2024:0499)
242766 Red Hat Update for libssh (RHSA-2024:0538)
242805 Red Hat Update for openssh (RHSA-2024:0606)
242811 Red Hat Update for libssh (RHSA-2024:0625)
242814 Red Hat Update for libssh (RHSA-2024:0628)
242828 Red Hat Update for openssh (RHSA-2024:0594)
242841 Red Hat Update for openssh (RHSA-2024:0455)
242848 Red Hat Update for openssh (RHSA-2024:0429)
242989 Red Hat OpenShift Container Platform 4.15 Security Update (RHSA-2023:7201)
243017 Red Hat Update for openssh (RHSA-2024:1130)

243033 Red Hat Update for buildah (RHSA-2024:1150)
243042 Red Hat Update for JBoss Enterprise Application Platform 8.0.1 (RHSA-2024:1193)
243043 Red Hat Update for JBoss Enterprise Application Platform 7.4 (RHSA-2024:1196)
243044 Red Hat Update for JBoss Enterprise Application Platform 8.0.1 (RHSA-2024:1192)
243173 Red Hat Update for JBoss Enterprise Application Platform 7.4.1 (RHSA-2024:1676)
243174 Red Hat Update for JBoss Enterprise Application Platform 7.4.1 (RHSA-2024:1675)
243175 Red Hat Update for JBoss Enterprise Application Platform 7.4.1 (RHSA-2024:1674)
284839 Fedora Security Update for podman (FEDORA-2023-cb8c606fbb)
284840 Fedora Security Update for proftpd (FEDORA-2023-b87ec6cf47)
284849 Fedora Security Update for putty (FEDORA-2024-71c2c6526c)
284850 Fedora Security Update for python (FEDORA-2024-39a8c72ea9)
284862 Fedora Security Update for golang (FEDORA-2024-ae653fb07b)
284864 Fedora Security Update for golang (FEDORA-2024-2705241461)
284870 Fedora Security Update for podman (FEDORA-2024-06ebb70bdd)
284889 Fedora Security Update for prometheus (FEDORA-2024-3fd1bc9276)
285023 Fedora Security Update for prometheus (FEDORA-2024-a53b24023d)
285053 Fedora Security Update for golang (FEDORA-2024-fb32950d11)
285055 Fedora Security Update for golang (FEDORA-2024-7b08207cdb)
285066 Fedora Security Update for podman (FEDORA-2024-3bb23c77f3)
285068 Fedora Security Update for putty (FEDORA-2024-d946b9ad25)
285075 Fedora Security Update for python (FEDORA-2023-e77300e4b5)
285076 Fedora Security Update for proftpd (FEDORA-2023-153404713b)
285080 Fedora Security Update for podman (FEDORA-2023-20feb865d8)
285088 Fedora Security Update for libssh (FEDORA-2023-0733306be9)
296108 Oracle Solaris 11.4 Support Repository Update (SRU) 66.164.1 Missing (CPUJAN2024)
330166 IBM Advanced Interactive eXecutive (AIX) Multiple Vulnerabilities (openssh_advisory16)
356793 Amazon Linux Security Advisory for openssh : ALAS2-2023-2376
356794 Amazon Linux Security Advisory for openssh : ALAS2023-2023-462
356795 Amazon Linux Security Advisory for openssh : ALAS-2023-1898

356999 Amazon Linux Security Advisory for openssh : AL2012-2023-483
379295 Putty Terrapin Attack SSH Connection Weakening Vulnerability
379302 Windows Secure Copy (WinSCP) Security Update
379344 Alibaba Cloud Linux Security Update for libssh (ALINUX3-SA-2024:0014)
379366 Fortinet FortiAnalyzer and FortiManager - Improper Access Control Vulnerability (FG-IR-23-490)
379473 Jenkins Plugins Multiple Security Vulnerabilities (Jenkins Security Advisory 2024-03-06)
379478 Apple macOS Sonoma 14.4 Not Installed (HT214084)
38913 SSH Prefix Truncation Vulnerability (Terrapin)
44169 Juniper Network Operating System (Junos OS) Terrapin Attack SSH Connection Weakening Vulnerability (JSA76462)
503807 Alpine Linux Security Update for dropbear
503809 Alpine Linux Security Update for libssh2
503855 Alpine Linux Security Update for proftpd
503904 Alpine Linux Security Update for dropbear
504326 Alpine Linux Security Update for putty
505868 Alpine Linux Security Update for dropbear
505888 Alpine Linux Security Update for libssh2
505902 Alpine Linux Security Update for openssh
505986 Alpine Linux Security Update for buildah
506001 Alpine Linux Security Update for doctl
506043 Alpine Linux Security Update for erlang
506053 Alpine Linux Security Update for filezilla
506076 Alpine Linux Security Update for gitea
506112 Alpine Linux Security Update for libssh
506157 Alpine Linux Security Update for pijul
506158 Alpine Linux Security Update for podman-tui
506161 Alpine Linux Security Update for podman
506169 Alpine Linux Security Update for py3-asyncssh
506178 Alpine Linux Security Update for py3-paramiko

506261 Alpine Linux Security Update for tinyssh
510674 Alpine Linux Security Update for nebula
510681 Alpine Linux Security Update for openssh
510754 Alpine Linux Security Update for openssh
510755 Alpine Linux Security Update for putty
6000398 Debian Security Update for openssh (DSA 5586-1)
6000402 Debian Security Update for putty (DSA 5588-1)
6000403 Debian Security Update for openssh (DLA 3694-1)
6000408 Debian Security Update for libssh (DSA 5591-1)
6000430 Debian Security Update for php-phpseclib3 (DSA 5601-1)
6000431 Debian Security Update for phpseclib (DSA 5599-1)
6000432 Debian Security Update for php-phpseclib (DSA 5600-1)
6000445 Debian Security Update for php-phpseclib (DLA 3718-1)
6000446 Debian Security Update for phpseclib (DLA 3719-1)
6000460 Debian Security Update for python-asyncssh (DLA 3730-1)
673335 EulerOS Security Update for libssh (EulerOS-SA-2024-1316)
673339 EulerOS Security Update for libssh2 (EulerOS-SA-2024-1217)
673381 EulerOS Security Update for libssh (EulerOS-SA-2024-1338)
673413 EulerOS Security Update for openssh (EulerOS-SA-2024-1183)
673430 EulerOS Security Update for proftpd (EulerOS-SA-2024-1323)
673454 EulerOS Security Update for libssh2 (EulerOS-SA-2024-1239)
673471 EulerOS Security Update for libssh2 (EulerOS-SA-2024-1339)
673472 EulerOS Security Update for libssh (EulerOS-SA-2024-1197)
673543 EulerOS Security Update for proftpd (EulerOS-SA-2024-1222)
673551 EulerOS Security Update for libssh2 (EulerOS-SA-2024-1317)
673621 EulerOS Security Update for proftpd (EulerOS-SA-2024-1244)
673655 EulerOS Security Update for openssh (EulerOS-SA-2024-1203)
673667 EulerOS Security Update for python-paramiko (EulerOS-SA-2024-1224)
673686 EulerOS Security Update for proftpd (EulerOS-SA-2024-1345)

673750 EulerOS Security Update for libssh (EulerOS-SA-2024-1216)
673780 EulerOS Security Update for libssh2 (EulerOS-SA-2024-1178)
673785 EulerOS Security Update for libssh (EulerOS-SA-2024-1177)
673788 EulerOS Security Update for openssh (EulerOS-SA-2024-1321)
673811 EulerOS Security Update for openssh (EulerOS-SA-2024-1286)
673872 EulerOS Security Update for openssh (EulerOS-SA-2024-1343)
673894 EulerOS Security Update for openssh (EulerOS-SA-2024-1241)
673897 EulerOS Security Update for libssh2 (EulerOS-SA-2024-1198)
673937 EulerOS Security Update for openssh (EulerOS-SA-2024-1219)
673955 EulerOS Security Update for python-paramiko (EulerOS-SA-2024-1246)
674082 EulerOS Security Update for libssh (EulerOS-SA-2024-1238)
691379 Free Berkeley Software Distribution (FreeBSD) Security Update for putty (91955195-9ebb-11ee-bc14-a703705db3a6)
691381 Free Berkeley Software Distribution (FreeBSD) Security Update for nebula (0f7598cc-9fe2-11ee-b47f-901b0e9408dc)
691386 Free Berkeley Software Distribution (FreeBSD) Security Update for Free Berkeley Software Distribution (FreeBSD) (13d83980-9f18-11ee-8e38-002590c1f29c)
691404 Free Berkeley Software Distribution (FreeBSD) Security Update for rclone (b5e22ec5-bc4b-11ee-b0b5-b42e991fc52e)
710817 Gentoo Linux libssh Multiple Vulnerabilities (GLSA 202312-16)
710818 Gentoo Linux OpenSSH Multiple Vulnerabilities (GLSA 202312-17)
731307 Palo Alto Networks (PAN-OS) Impact of Terrapin SSH Attack Vulnerability (PAN-241547, CGSDW-19542)
755496 SUSE Enterprise Linux Security Update for openssh (SUSE-SU-2023:4905-1)
755497 SUSE Enterprise Linux Security Update for openssh (SUSE-SU-2023:4904-1)
755498 SUSE Enterprise Linux Security Update for openssh (SUSE-SU-2023:4903-1)
755499 SUSE Enterprise Linux Security Update for openssh (SUSE-SU-2023:4902-1)
755517 SUSE Enterprise Linux Security Update for libssh2_org (SUSE-SU-2023:4946-1)
755553 SUSE Enterprise Linux Security Update for libssh2_org (SUSE-SU-2024:0006-1)
755579 SUSE Enterprise Linux Security Update for python-paramiko (SUSE-SU-2024:0035-1)
755645 SUSE Enterprise Linux Security Update for erlang (SUSE-SU-2024:0210-1)
755655 SUSE Enterprise Linux Security Update for apache-parent, apache-sshd (SUSE-SU-2024:0224-1)
755708 SUSE Enterprise Linux Security Update for bouncycastle, jsch (SUSE-SU-2024:0327-1)

755732 SUSE Enterprise Linux Security Update for cosign (SUSE-SU-2024:0430-1)
755745 SUSE Enterprise Linux Security Update for rekor (SUSE-SU-2024:0460-1)
755791 SUSE Enterprise Linux Security Update for libssh2_org (SUSE-SU-2024:0543-1)
755792 SUSE Enterprise Linux Security Update for libssh2_org (SUSE-SU-2024:0558-1)
755806 SUSE Enterprise Linux Security Update for libssh (SUSE-SU-2024:0539-1)
755989 SUSE Enterprise Linux Security Update for jsch-agent-proxy (SUSE-SU-2024:0974-1)
755991 SUSE Enterprise Linux Security Update for jbcrypt, trilead-ssh2 (SUSE-SU-2024:0972-1)
770234 Red Hat OpenShift Container Platform 4.15 Security Update (RHSA-2023:7201)
907717 Common Base Linux Mariner (CBL-Mariner) Security Update for libssh (32200-1)
907796 Common Base Linux Mariner (CBL-Mariner) Security Update for jsch (32259-2)
907806 Common Base Linux Mariner (CBL-Mariner) Security Update for openssh (32204-1)
907822 Common Base Linux Mariner (CBL-Mariner) Security Update for moby-engine (32280-2)
907868 Common Base Linux Mariner (CBL-Mariner) Security Update for moby-cli (32223-1)
907970 Common Base Linux Mariner (CBL-Mariner) Security Update for erlang (32196-1)
907979 Common Base Linux Mariner (CBL-Mariner) Security Update for libssh2 (32201-1)
907980 Common Base Linux Mariner (CBL-Mariner) Security Update for cert-manager (32195-1)
907991 Common Base Linux Mariner (CBL-Mariner) Security Update for nmap (32202-1)
941560 AlmaLinux Security Update for openssh (ALSA-2024:0606)
941563 AlmaLinux Security Update for libssh (ALSA-2024:0628)
941611 AlmaLinux Security Update for buildah (ALSA-2024:1150)
941612 AlmaLinux Security Update for openssh (ALSA-2024:1130)
961110 Rocky Linux Security Update for openssh (RLSA-2024:0606)
961112 Rocky Linux Security Update for libssh (RLSA-2024:0628)
996349 GO (Go) Security Update for golang.org/x/crypto (GHSA-45x7-px36-x8w8)
996375 Rust (Rust) Security Update for golang.org/x/crypto (GHSA-45x7-px36-x8w8)
996391 Python (Pip) Security Update for golang.org/x/crypto (GHSA-45x7-px36-x8w8)

this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)