CVE-2023-25136

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2023-25136
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-02-03 06:15:00 UTC
Updated	2023-11-07 04:08:00 UTC
Description	OpenSSH server (sshd) 9.1 introduced a double-free vulnerability during options.kex_algorithms handling. This is fixed in C

Risk And Classification

Problem Types: CWE-415

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	37	All	All	All
Operating System	Fedoraproject	Fedora	38	All	All	All
Hardware	Netapp	500f	-	All	All	All
Operating System	Netapp	500f Firmware	-	All	All	All
Hardware	Netapp	A250	-	All	All	All
Operating System	Netapp	A250 Firmware	-	All	All	All
Hardware	Netapp	C250	-	All	All	All
Operating System	Netapp	C250 Firmware	-	All	All	All
Application	Netapp	Ontap Select Deploy Administration Utility	-	All	All	All
Application	Openssh	Openssh	9.1	All	All	All

References

Reference	Source	Link
3522 – Crash with "free(): double free detected" with old clients	MISC	bugzilla.min
[SECURITY] Fedora 37 Update: openssh-8.8p1-10.fc37 - package-announce - Fedora Mailing-Lists		lists.fedorap
CVE-2023-25136 OpenSSH Vulnerability in NetApp Products | NetApp Product Security	CONFIRM	security.neta
[SECURITY] Fedora 38 Update: openssh-9.0p1-15.fc38 - package-announce - Fedora Mailing-Lists		lists.fedorap

oss-security - Re: Re: double-free vulnerability in OpenSSH server 9.1 (CVE-2023-25136)	MLIST	www.openw
oss-security - Re: double-free vulnerability in OpenSSH server 9.1 (CVE-2023-25136)	MLIST	www.openw
CVE-2023-25136 OpenSSH Pre-Auth Double Free Writeup & PoC	MISC	jfrog.com
[SECURITY] Fedora 37 Update: openssh-8.8p1-10.fc37 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedorap
OpenSSH Pre-Auth Double Free – CVE-2023-25136 – Writeup and Proof-of-Concept | Hacker News	MISC	news.ycomb
oss-security - Re: Re: double-free vulnerability in OpenSSH server 9.1 (CVE-2023-25136)	MLIST	www.openw
oss-security - Re: double-free vulnerability in OpenSSH server 9.1 (CVE-2023-25136)	MLIST	www.openw
upstream: Always return allocated strings from the kex filtering so · openssh/openssh-portable@486c4dc · GitHub	MISC	github.com
oss-security - double-free vulnerability in OpenSSH server 9.1	MISC	www.openw
oss-security - Re: Re: double-free vulnerability in OpenSSH server 9.1 (CVE-2023-25136)	MLIST	www.openw
[SECURITY] Fedora 38 Update: openssh-9.0p1-15.fc38 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedorap
oss-security - Re: Re: double-free vulnerability in OpenSSH server 9.1 (CVE-2023-25136)	MLIST	www.openw
OpenSSH: Remote Code Execution (GLSA 202307-01) — Gentoo security	GENTOO	security.gen
ftp.openbsd.org/pub/OpenBSD/patches/7.2/common/017_sshd.patch.sig	MISC	ftp.openbsd
CVE Program record	CVE.ORG	www.cve.or
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- 160641 Oracle Enterprise Linux Security Update for openssh (ELSA-2023-2645)
- 184729 Debian Security Update for openssh (CVE-2023-25136)
- 241463 Red Hat Update for openssh (RHSA-2023:2645)
- 283896 Fedora Security Update for openssh (FEDORA-2023-1176c8b10c)
- 284173 Fedora Security Update for openssh (FEDORA-2023-123647648e)
- 38888 OpenSSH server 9.1 'sshd(8)' Double-Free Vulnerability
- 673019 EulerOS Security Update for openssh (EulerOS-SA-2023-1981)
- 673022 EulerOS Security Update for openssh (EulerOS-SA-2023-1959)
- 710742 Gentoo Linux OpenSSH Remote Code Execution (RCE) Vulnerability (GLSA 202307-01)
- 905383 Common Base Linux Mariner (CBL-Mariner) Security Update for openssh (13208)
- 905384 Common Base Linux Mariner (CBL-Mariner) Security Update for openssh (13213)
- 941047 AlmaLinux Security Update for openssh (ALSA-2023:2645)