



# CVE-2023-25136

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

## Summary

<b>CVE</b>	CVE-2023-25136
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-02-03 06:15:00 UTC
<b>Updated</b>	2023-11-07 04:08:00 UTC
<b>Description</b>	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	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	37	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	38	All	All	All
Hardware	<a href="#">Netapp</a>	<a href="#">500f</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">500f Firmware</a>	-	All	All	All
Hardware	<a href="#">Netapp</a>	<a href="#">A250</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">A250 Firmware</a>	-	All	All	All
Hardware	<a href="#">Netapp</a>	<a href="#">C250</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">C250 Firmware</a>	-	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Ontap Select Deploy Administration Utility</a>	-	All	All	All
Application	<a href="#">Openssh</a>	<a href="#">Openssh</a>	9.1	All	All	All

## References

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

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

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)

---

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to 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](#)**