



CVE-2023-1667

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

Summary

CVE	CVE-2023-1667
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-05-26 18:15:00 UTC
Updated	2023-12-22 10:15:00 UTC
Description	A NULL pointer dereference was found In libssh during re-keying with algorithm guessing. This issue may allow an authenti

Risk And Classification

Problem Types: CWE-476

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Fedoraproject	Fedora	37	All	All	All
Application	Libssh	Libssh	All	All	All	All
Application	Libssh	Libssh	All	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Operating System	Redhat	Enterprise Linux	9.0	All	All	All

References

Reference	Source	Link
2182199 – (CVE-2023-1667) CVE-2023-1667 libssh: NULL pointer dereference during rekeying with algorithm guessing	MISC	bugzi
www.libssh.org/security/advisories/CVE-2023-1667.txt	MISC	www.
[SECURITY] Fedora 37 Update: libssh-0.10.5-1.fc37 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fe
[SECURITY] [DLA 3437-1] libssh security update	MLIST	lists.d
cve-details	MISC	acce
libssh: Multiple Vulnerabilities (GLSA 202312-05) — Gentoo security		secur
[SECURITY] Fedora 37 Update: libssh-0.10.5-1.fc37 - package-announce - Fedora Mailing-Lists		lists.fe
CVE Program record	CVE.ORG	www.

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

160756 Oracle Enterprise Linux Security Update for libssh (ELSA-2023-3839)
161111 Oracle Enterprise Linux Security Update for libssh (ELSA-2023-6643)
181800 Debian Security Update for libssh (DSA 5409-1)
181812 Debian Security Update for libssh (DLA 3437-1)
184794 Debian Security Update for libssh (CVE-2023-1667)
199393 Ubuntu Security Notification for libssh Vulnerabilities (USN-6138-1)
241759 Red Hat Update for libssh (RHSA-2023:3839)
242284 Red Hat Update for libssh (RHSA-2023:6643)
242766 Red Hat Update for libssh (RHSA-2024:0538)
284002 Fedora Security Update for libssh (FEDORA-2023-5fa5ca2043)
284140 Fedora Security Update for libssh (FEDORA-2023-741d5f1fd3)
355399 Amazon Linux Security Advisory for libssh : ALAS2023-2023-186
378712 Alibaba Cloud Linux Security Update for libssh (ALINUX3-SA-2023:0077)
673239 EulerOS Security Update for libssh (EulerOS-SA-2023-2358)
673258 EulerOS Security Update for libssh (EulerOS-SA-2023-2384)
673285 EulerOS Security Update for libssh (EulerOS-SA-2023-2586)
673294 EulerOS Security Update for libssh (EulerOS-SA-2023-2616)
673826 EulerOS Security Update for libssh (EulerOS-SA-2023-2693)
673847 EulerOS Security Update for libssh (EulerOS-SA-2023-2651)
710806 Gentoo Linux libssh Multiple Vulnerabilities (GLSA 202312-05)
755806 SUSE Enterprise Linux Security Update for libssh (SUSE-SU-2024:0539-1)
941161 AlmaLinux Security Update for libssh (ALSA-2023:3839)
941363 AlmaLinux Security Update for libssh (ALSA-2023:6643)
960954 Rocky Linux Security Update for libssh (RLSA-2023:3839)

© [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](#)