Libssh: memory exhaustion via repeated key exchange in libssh

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2025-8277
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-09-09 12:15:30 UTC
Updated	2026-05-06 16:16:04 UTC
Description	A flaw was found in libssh's handling of key exchange (KEX) processes when a client repeatedly sends incorrect KEX gues

Risk And Classification

Primary CVSS: v3.1 3.1 LOW from secalert@redhat.com

CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:L

Problem Types: CWE-401 | CWE-401 Missing Release of Memory after Effective Lifetime

Version	Source	Type	Score	Severity	Vector
3.1	secalert@redhat.com	Secondary	3.1	LOW	CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:L
3.1	CNA	CVSS	3.1	LOW	CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:L

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

Low

CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:L

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Red Hat	Red Hat Enterprise Linux 10	Not specified	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 6	Not specified	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 7	Not specified	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 8	Not specified	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 9	Not specified	Not specified
CNA	Red Hat	Red Hat OpenShift Container Platform 4	Not specified	Not specified

References

Reference	Source	Link	Tags
www.libssh.org/security/advisories/CVE-2025-8277.txt	secalert@redhat.com	www.libssh.org	
bugzilla.redhat.com/show_bug.cgi	secalert@redhat.com	bugzilla.redhat.com	
access.redhat.com/security/cve/CVE-2025-8277	secalert@redhat.com	access.redhat.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

CNA: Red Hat would like to thank Francesco Rollo for reporting this issue. (en)

Additional Advisory Data

Source	Time	Event
CNA	2025-07-28T11:01:26.808Z	Reported to Red Hat.
CNA	2025-09-09T00:00:00.000Z	Made public.

Workarounds

CNA: Mitigation for this issue is either not available or the currently available options don't meet the Red Hat Product Security criteria comprising ease of use and deployment, applicability to widespread installation base, or stability. It is strongly advised to apply updated libssh packages once available to prevent memory exhaustion risks on client systems.

There are currently no legacy QID mappings associated with this CVE.

There are currently no legacy CVE mappings associated with this CVE.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**