



Malicious Key Exchange Messages may Lead to Excessive Resource Consumption

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

Summary

CVE	CVE-2025-48040
State	PUBLISHED
Assigner	EEF
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-09-11 09:15:34 UTC
Updated	2026-04-06 17:17:03 UTC
Description	Uncontrolled Resource Consumption vulnerability in Erlang OTP ssh (ssh_sftp modules) allows Excessive Allocation, Floo

Risk And Classification

Primary CVSS: v4.0 6.9 MEDIUM from 6b3ad84c-e1a6-4bf7-a703-f496b71e49db

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:L/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Problem Types: CWE-400 | CWE-770 | CWE-400 CWE-400 Uncontrolled Resource Consumption | CWE-770 CWE-770 Allocation of Resources Without Limits or Throttling

Version	Source	Type	Score	Severity	Vector
4.0	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	Secondary	6.9	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:
4.0	CNA	CVSS	6.9	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

None

Integrity

None

Availability

Low

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:L/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Erlang	OTP	affected 3.0.1 * otp	Not specified
CNA	Erlang	OTP	affected 17.0 * otp	Not specified
CNA	Erlang	OTP	affected 07b8f441ca711f9812fad9e9115bab3c3aa92f79 * git	Not specified

References

Reference	Source	Link
osv.dev/vulnerability/EEF-CVE-2025-48040	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	osv.dev
github.com/erlang/otp/security/advisories/GHSA-h7rg-6rjg-4cph	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	github.com
github.com/erlang/otp/pull/10162	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	github.com
www.erlang.org/doc/system/versions.html	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	www.erlang.org
github.com/erlang/otp/commit/548f1295d86d0803da884db8685cc16d461d0d5a	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	github.com
github.com/erlang/otp/commit/7cd7abb7e19e16b027eaae6a54e1f6fbb21181a	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	github.com
cna.erlef.org/cves/CVE-2025-48040.html	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	cna.erlef.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

CNA: Jakub Witczak (en)

CNA: Ingela Andin (en)

Workarounds

CNA: * set option parallel_login to false * reduce max_sessions option

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

© [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](#)