SSH_FXP_OPENDIR may Lead to Exhaustion of File Handles

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2025-48041
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	Allocation of Resources Without Limits or Throttling vulnerability in Erlang OTP ssh (ssh_sftp modules) allows Excessive Al

Risk And Classification

Primary CVSS: v4.0 7.1 HIGH from 6b3ad84c-e1a6-4bf7-a703-f496b71e49db

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:N/VI:N/VA:H/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/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

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

Version	Source	Type	Score	Severity	Vector
4.0	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	Secondary	7.1	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:N/VI:N/VA:H
4.0	CNA	CVSS	7.1	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:N/VI:N/VA:H

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

Low

User Interaction

None

Confidentiality

None

ntegrity

None

Availability

High

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:N/VI:N/VA:H/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/MSC:X/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
github.com/erlang/otp/security/advisories/GHSA-79c4-cvv7-4qm3	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	github.com
github.com/erlang/otp/pull/10157	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/5f9af63eec4657a37663828d206517828cb9f288	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	github.com
github.com/erlang/otp/commit/d49efa2d4fa9e6f7ee658719cd76ffe7a33c2401	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	github.com
cna.erlef.org/cves/CVE-2025-48041.html	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	cna.erlef.org
osv.dev/vulnerability/EEF-CVE-2025-48041	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	osv.dev
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)

Additional Advisory Data

Workarounds

CNA: * disabling SFTP * limiting number of max_sessions allowed for sshd, so exploiting becomes more complicated

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