CVE-2025-48041

SSH_FXP_OPENDIR may Lead to Exhaustion of File Handles

« Back to all CVEs

See on OSV.dev »

Weakness Type (CWE)

CWE-770 — CWE-770 Allocation of Resources Without Limits or Throttling

CAPEC

CAPEC-130 — CAPEC-130 Excessive Allocation
CAPEC-125 — CAPEC-125 Flooding

CVSS 4.0 Score

7.1

HIGH

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

Vulnerability description

Allocation of Resources Without Limits or Throttling vulnerability in Erlang OTP ssh (ssh_sftp modules) allows Excessive Allocation, Flooding.
This vulnerability is associated with program files `lib/ssh/src/ssh_sftpd.erl`.

This issue affects OTP form OTP 17.0 until OTP 28.0.3, OTP 27.3.4.3 and 26.2.5.15 corresponding to ssh from 3.0.1 until 5.3.3, 5.2.11.3 and 5.1.4.12.

Affected

`pkg:otp/ssh`

Module	Source File
ssh_sftp	lib/ssh/src/ssh_sftpd.erl

Status	Type	Version	Changes / Fixed in
Affected	otp ⓘ	3.0.1	• unaffected at 5.3.3 • unaffected at 5.2.11.3 • unaffected at 5.1.4.12

pkg:github/erlang/otp

Module	Source File
ssh_sftp	lib/ssh/src/ssh_sftpd.erl

Status	Type	Version	Changes / Fixed in
Affected	otp ⓘ	17.0	• unaffected at 28.0.3 • unaffected at 27.3.4.3 • unaffected at 26.2.5.15
Affected	git ⓘ	07b8f441ca71	• unaffected at 5f9af63eec46 • unaffected at d49efa2d4fa9

Configurations

The SFTP subsystem must be enabled on the SSH server and the SSH port must be reachable by the attacker. SFTP is enabled by default unless explicitly disabled by setting `{subsystems, []}` in the SSH daemon configuration.

Workarounds

- disabling SFTP
- limiting number of `max_sessions` allowed for `sshd`, so exploiting becomes more complicated

References

- https://github.com/erlang/otp/security/advisories/GHSA-79c4-cvv7-4qm3 **vendor-advisory** **related**
- https://osv.dev/vulnerability/EEF-CVE-2025-48041 **related**
- https://github.com/erlang/otp/pull/10157 **patch**
- https://github.com/erlang/otp/commit/5f9af63eec4657a37663828d206517828cb9f288 **patch**
- https://github.com/erlang/otp/commit/d49efa2d4fa9e6f7ee658719cd76ffe7a33c2401 **patch**

Credits

- **Remediation developer**: Jakub Witczak
- **Remediation reviewer**: Ingela Andin

CVE record as JSON: `GET /cves/CVE-2025-48041.json`
OSV record as JSON: `GET /osv/EEF-CVE-2025-48041.json`