



EEF-CVE- 2025-48039

[See a problem?](#)

Please try reporting it [to the source](#) [↗](#) first.

Source	https://cna.erlef.org/osv/EEF-CVE-2025-48039.html ↗
Import Source	https://cna.erlef.org/osv/EEF-CVE-2025-48039.json ↗
JSON Data	https://api.osv.dev/v1/vulns/EEF-CVE-2025-48039 ↗
Aliases	CVE-2025-48039 GHSA-rr5p-6856-j7h8
Published	2025-09-11T08:13:36.878Z
Modified	2026-04-07T15:00:14.897384Z
Severity	5.3 (Medium) CVSS_V4 - CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:N/VI:N/VA:L/SC:N/SI:N/SA:N CVSS Calculator ↗

Summary Unverified Paths can Cause Excessive Use of System Resources

Details

Summary

Allocation of Resources Without Limits or Throttling vulnerability in Erlang OTP ssh (*sshsftp modules*) allows *Excessive Allocation, Resource Leak Exposure*. This vulnerability is associated with program files *lib/ssh/src/sshsftpd.erl*.

This issue affects OTP from 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.

Workaround

- Disable sftp
 - limiting number of max_sessions allowed for sshd, so exploiting becomes more complicated

Configuration

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.

```
Database specific ↗ {
  "capec_ids": [
    "CAPEC-130",
    "CAPEC-131"
  ],
  "cpe_ids": [
    "cpe:2.3:a:erlang:erlang\\\/otp:*:*:*:*:*:*:*"
  ],
  "cwe_ids": [
    "CWE-770",
    "CWE-400"
  ]
}
```

References

<https://github.com/erlang/otp/security/advisories/GHSA-rr5p-6856-j7h8> [↗](#)

<https://cna.erlef.org/cves/CVE-2025-48039.html> [↗](#)

<https://www.erlang.org/doc/system/versions.html#order-of-versions> [↗](#)

<https://github.com/erlang/otp/pull/10155> [↗](#)

<https://github.com/erlang/otp/commit/c242e6458967e9514bea351814151695807a54ac> [↗](#)

<https://github.com/erlang/otp/commit/043ee3c943e2977c1acdd740ad13992fd60b6bf0> [↗](#)

Credits

Jakub Witczak - REMEDIATION_DEVELOPER

Ingela Andin - REMEDIATION_REVIEWER

Affected packages

Git
github.com/erlang/otp

Affected ranges [↗](#)

Type GIT

Repo <https://github.com/erlang/otp>


Events Introduced

[07b8f441ca711f9812fad9e9115bab3c3aa92f79](https://github.com/erlang/otp/commit/07b8f441ca711f9812fad9e9115bab3c3aa92f79) [↗](#)

Fixed

[c242e6458967e9514bea351814151695807a54ac](https://github.com/erlang/otp/commit/c242e6458967e9514bea351814151695807a54ac) [↗](#)

Fixed

[043ee3c943e2977c1acdd740ad13992fd60b6bf0](#) 

Affected versions

- ▶ OTP-17.*
 - ▶ OTP-18.*
 - ▶ OTP-19.*
 - ▶ OTP-20.*
 - ▶ OTP-21.*
 - ▶ OTP-22.*
 - ▶ OTP-23.*
 - ▶ OTP-24.*
 - ▶ OTP-25.*
 - ▶ OTP-26.*
 - ▶ OTP-27.*
 - ▶ OTP-28.*
 - ▶ Other
-

Database specific

- ▶ source
-

