EEF-CVE-2025-48038

See a problem?
Please try reporting it to the source first.

Source	https://cna.erlef.org/osv/EEF-CVE-2025-48038.html
Import Source	https://cna.erlef.org/osv/EEF-CVE-2025-48038.json
JSON Data	https://api.osv.dev/v1/vulns/EEF-CVE-2025-48038
Aliases	CVE-2025-48038 GHSA-pvj7-9652-7h9r
Published	2025-09-11T08:13:04.030Z
Modified	2026-04-07T15:00:17.059286Z
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 File Handles can Cause Excessive Use of System Resources
Details	

Summary

Allocation of Resources Without Limits or Throttling vulnerability in Erlang OTP ssh (ssh*sftp modules) allows Excessive Allocation, Resource Leak Exposure. 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.

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


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


References

https://github.com/erlang/otp/security/advisories/GHSA-pvj7-9652-7h9r

https://cna.erlef.org/cves/CVE-2025-48038.html

https://www.erlang.org/doc/system/versions.html#order-of-versions

https://github.com/erlang/otp/pull/10156

https://github.com/erlang/otp/commit/4e3bf86777ab3db7220c11d8ddabf15970ddd10a

https://github.com/erlang/otp/commit/f09e0201ff701993dc24a08f15e524daf72db42f

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
Fixed
4e3bf86777ab3db7220c11d8ddabf15970ddd10a

Fixed
f09e0201ff701993dc24a08f15e524daf72db42f

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