EEF-CVE-2025-48041

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

Source	https://cna.erlef.org/osv/EEF-CVE-2025-48041.html
Import Source	https://cna.erlef.org/osv/EEF-CVE-2025-48041.json
JSON Data	https://api.osv.dev/v1/vulns/EEF-CVE-2025-48041
Aliases	CVE-2025-48041 GHSA-79c4-cvv7-4qm3
Published	2025-09-11T08:14:20.508Z
Modified	2026-04-07T15:00:15.620953Z
Severity	7.1 (High) CVSS_V4 - 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 CVSS Calculator
Summary	SSH_FXP_OPENDIR may Lead to Exhaustion of File Handles
Details	

Summary

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.

Workaround

- disabling 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-125"
    ],
    "cpe_ids": [
        "cpe:2.3:a:erlang:erlang\\/otp:*:*:*:*:*:*:*:*"
    ],
    "cwe_ids": [
        "CWE-770",
        "CWE-400"
    ]
}
```


References

https://github.com/erlang/otp/security/advisories/GHSA-79c4-cvv7-4qm3

https://cna.erlef.org/cves/CVE-2025-48041.html

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

https://github.com/erlang/otp/pull/10157

https://github.com/erlang/otp/commit/5f9af63eec4657a37663828d206517828cb9f288

https://github.com/erlang/otp/commit/d49efa2d4fa9e6f7ee658719cd76ffe7a33c2401

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
5f9af63eec4657a37663828d206517828cb9f288

Fixed
d49efa2d4fa9e6f7ee658719cd76ffe7a33c2401

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