



# EEF-CVE- 2025-48041

[See a problem?](#)

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

Source	<a href="https://cna.erlef.org/osv/EEF-CVE-2025-48041.html">https://cna.erlef.org/osv/EEF-CVE-2025-48041.html</a> <a href="#">↗</a>
Import Source	<a href="https://cna.erlef.org/osv/EEF-CVE-2025-48041.json">https://cna.erlef.org/osv/EEF-CVE-2025-48041.json</a> <a href="#">↗</a>
JSON Data	<a href="https://api.osv.dev/v1/vulns/EEF-CVE-2025-48041">https://api.osv.dev/v1/vulns/EEF-CVE-2025-48041</a> <a href="#">↗</a>
Aliases	<a href="#">CVE-2025-48041</a> <a href="#">GHSA-79c4-cv7-4qm3</a>
Published	2025-09-11T08:14:20.508Z
Modified	2026-04-07T15:00:15.620953Z
Severity	<b>7.1 (High)</b> 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 <a href="#">CVSS Calculator</a> <a href="#">↗</a>

**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` (`sshsftp` modules) allows Excessive Allocation, Flooding. 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

- 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 ↗ {
  "cwe_ids": [
    "CWE-770",
    "CWE-400"
  ],
  "capec_ids": [
    "CAPEC-130",
    "CAPEC-125"
  ],
  "cpe_ids": [
    "cpe:2.3:a:erlang:erlang\\\/otp:*:*:*:*:*:*:*"
  ]
}
```

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](https://github.com/erlang/otp)

### Affected ranges [↗](#)

Type	GIT
Repo	<a href="https://github.com/erlang/otp">https://github.com/erlang/otp</a>
Events	Introduced <a href="https://github.com/erlang/otp/commit/07b8f441ca711f9812fad9e9115bab3c3aa92f79">07b8f441ca711f9812fad9e9115bab3c3aa92f79</a> <a href="#">↗</a>
	Fixed <a href="https://github.com/erlang/otp/commit/5f9af63eec4657a37663828d206517828cb9f288">5f9af63eec4657a37663828d206517828cb9f288</a> <a href="#">↗</a>

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
-

