# Pre-auth SSH DoS via unbounded zlib inflate

MITRE | NVD | CVE.ORG | Print: PDF

## Summary

| | |
|---|---|
| **CVE** | CVE-2026-23943 |
| **State** | PUBLISHED |
| **Assigner** | EEF |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2026-03-13 19:54:15 UTC |
| **Updated** | 2026-04-06 17:17:08 UTC |
| **Description** | Improper Handling of Highly Compressed Data (Compression Bomb) vulnerability in Erlang OTP ssh (ssh_transport module |

## Risk And Classification

**Primary CVSS:** v4.0 6.9 MEDIUM from 6b3ad84c-e1a6-4bf7-a703-f496b71e49db

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:L/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

**Problem Types:** CWE-409 | CWE-409 CWE-409 Improper Handling of Highly Compressed Data (Data Amplification)

| Version | Source | Type | Score | Severity | Vector |
|---|---|---|---|---|---|
| 4.0 | 6b3ad84c-e1a6-4bf7-a703-f496b71e49db | Secondary | 6.9 | MEDIUM | CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA: |
| 4.0 | CNA | CVSS | 6.9 | MEDIUM | CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA: |

## CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

None

ntegrity

None

Availability

Low

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:L/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

## Vendor Declared Affected Products

| Source | Vendor | Product | Version | Platforms |
|---|---|---|---|---|
| CNA | Erlang | OTP | affected 3.0.1 * otp | Not specified |
| CNA | Erlang | OTP | affected 17.0 * otp | Not specified |
| CNA | Erlang | OTP | affected 07b8f441ca711f9812fad9e9115bab3c3aa92f79 * git | Not specified |

## References

| Reference | Source | Link |
|---|---|---|
| github.com/erlang/otp/commit/43a87b949bdff12d629a8c34146711d9da93b1b1 | 6b3ad84c-e1a6-4bf7-a703-f496b71e49db | github.com |
| github.com/erlang/otp/security/advisories/GHSA-c836-qprm-jw9r | 6b3ad84c-e1a6-4bf7-a703-f496b71e49db | github.com |
| www.erlang.org/doc/system/versions.html | 6b3ad84c-e1a6-4bf7-a703-f496b71e49db | www.erlang.org |
| osv.dev/vulnerability/EEF-CVE-2026-23943 | 6b3ad84c-e1a6-4bf7-a703-f496b71e49db | osv.dev |
| github.com/erlang/otp/commit/0c1c04b191f6ab940e8fcfabce39eb5a8a6440a4 | 6b3ad84c-e1a6-4bf7-a703-f496b71e49db | github.com |
| cna.erlef.org/cves/CVE-2026-23943.html | 6b3ad84c-e1a6-4bf7-a703-f496b71e49db | cna.erlef.org |
| github.com/erlang/otp/commit/93073c3bd338c60cd2bae715ce6a1d4ffc1a8fd3 | 6b3ad84c-e1a6-4bf7-a703-f496b71e49db | github.com |
| CVE Program record | CVE.ORG | www.cve.org |
| NVD vulnerability detail | NVD | nvd.nist.gov |

## Vendor Comments And Credit

Discovery Credit

**CNA:** Igor Morgenstern / Aisle Research (en)

**CNA:** Michał Wąsowski (en)

**CNA:** Jakub Witczak (en)

## Additional Advisory Data

Workarounds

**CNA:** Best workaround - Disable all compression: {preferred_algorithms, [{compression, ['none']}]} Alternative mitigations (less secure): * Disable only pre-auth zlib compression (authenticated users can still exploit via zlib@openssh.com): {modify_algorithms, [{rm, [{compression, ['zlib']}]}]} * Limit concurrent sessions (reduces attack surface but does not prevent exploitation): {max_sessions, N} % Cap total concurrent sessions (default is infinity)

There are currently no legacy QID mappings associated with this CVE.