



# Pre-auth SSH DoS via unbounded zlib inflate

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2026-23943
<b>State</b>	PUBLISHED
<b>Assigner</b>	EEF
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-03-13 19:54:15 UTC
<b>Updated</b>	2026-04-06 17:17:08 UTC
<b>Description</b>	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/MSX/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

Integrity

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/MSX/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	<a href="#">Erlang</a>	OTP	affected 3.0.1 * otp	Not specified
CNA	<a href="#">Erlang</a>	OTP	affected 17.0 * otp	Not specified
CNA	<a href="#">Erlang</a>	OTP	affected 07b8f441ca711f9812fad9e9115bab3c3aa92f79 * git	Not specified

### References

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

### Vendor Comments And Credit

Discovery Credit

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

**CNA:** Michał Wąsowski (en)

**CNA:** Jakub Witczak (en)

#### 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.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status [status.cve.report](#)**