



# CVE-2025-63261

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

## Summary

<b>CVE</b>	CVE-2025-63261
<b>State</b>	PUBLISHED
<b>Assigner</b>	mitre
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-03-20 21:17:12 UTC
<b>Updated</b>	2026-04-07 16:08:00 UTC
<b>Description</b>	AWStats 8.0 is vulnerable to Command Injection via the open function

## Risk And Classification

**Primary CVSS:** v3.1 7.8 HIGH from ADP

**CVSS:** 3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

**EPSS:** 0.000630000 probability, percentile 0.194540000 (date 2026-04-07)

**Problem Types:** CWE-78 | n/a | CWE-78 CWE-78 Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

Version	Source	Type	Score	Severity	Vector
3.1	ADP	DECLARED	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

## CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Awstats	Awstats	7.9	All	All	All
Operating System	Debian	Debian Linux	11.0	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	Source	Link	Tags
pentest-tools.com/PTT-2025-021-Code-Execution-in-AWStats.pdf	cve@mitre.org	pentest-tools.com	Exploit,
github.com/eldy/AWStats/blob/develop/wwwroot/cgi-bin/awstats.pl	cve@mitre.org	github.com	Produc
lists.debian.org/debian-lts-announce/2026/03/msg00013.html	af854a3a-2127-422b-91ae-364da2661108	lists.debian.org	Mailing
CVE Program record	CVE.ORG	www.cve.org	canonic
NVD vulnerability detail	NVD	nvd.nist.gov	canonic

No vendor comments have been submitted for this CVE.

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.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report