



Unauthenticated XML External Entity Injection in AOS-8 Instant allows Denial of Service

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

Summary

CVE CVE-2026-23822

State PUBLISHED

Assigner hpe

Source Priority CVE Program / NVD first with legacy fallback

Published 2026-05-12 19:16:28 UTC

Updated 2026-05-12 20:16:31 UTC

Description A vulnerability in the XML handling component of AOS-8 DHCP services could allow an unauthenticated remote attacker to

Risk And Classification

Primary CVSS: v3.1 5.3 MEDIUM from security-alert@hpe.com

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

Problem Types: CWE-776 | CWE-776 CWE-776 Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion')

Version	Source	Type	Score	Severity	Vector
3.1	security-alert@hpe.com	Secondary	5.3	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:N/A:H
3.1	CNA	CVSS	5.3	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:N/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Hewlett Packard Enterprise HPE	ArubaOS AOS	affected 8.13.0.0 8.13.1.1 semver	Not specified
CNA	Hewlett Packard Enterprise HPE	ArubaOS AOS	affected 8.12.0.0 8.12.0.6 semver	Not specified
CNA	Hewlett Packard Enterprise HPE	ArubaOS AOS	affected 8.10.0.0 8.10.0.21 semver	Not specified

References

Reference	Source	Link	Tags
support.hpe.com/hpesc/public/docDisplay	security-alert@hpe.com	support.hpe.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

CNA: [Nicholas Starke \(en\)](#)

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