Use after free when parsing EDNS options in Lua

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2026-27854
State	PUBLISHED
Assigner	OX
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-31 12:16:28 UTC
Updated	2026-04-01 14:24:02 UTC
Description	An attacker might be able to trigger a use-after-free by sending crafted DNS queries to a DNSdist using the DNSQuestion:g

Risk And Classification

Primary CVSS: v3.1 4.8 MEDIUM from security@open-xchange.com

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

EPSS: 0.000090000 probability, percentile 0.009440000 (date 2026-04-01)

Problem Types: CWE-416 | Use After Free | CWE-416 CWE-416 Use After Free

Version	Source	Type	Score	Severity	Vector
3.1	security@open-xchange.com	Secondary	4.8	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:L
3.1	CNA	CVSS	4.8	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:L

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

None

None

Availability

Low

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	PowerDNS	DNSdist	affected 1.9.0 1.9.12 semver	Not specified
CNA	PowerDNS	DNSdist	affected 2.0.0 2.0.3 semver	Not specified

References

Reference	Source	Link	Tags
www.dnsdist.org/security-advisories/powerdns-advisory-for-dnsdist-2026-02.html	security@open-xchange.com	www.dnsdist.org	
CVE Program record	CVE.ORG	www.cve.org	canonic
NVD vulnerability detail	NVD	nvd.nist.gov	canonic

Vendor Comments And Credit

Discovery Credit

CNA: Naoki Wakamatsu (en)

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