Crafted delegations or IP fragments can poison cached delegations in Recursor

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2025-59023
State	PUBLISHED
Assigner	OX
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-02-09 15:16:10 UTC
Updated	2026-04-20 15:11:13 UTC
Description	Crafted delegations or IP fragments can poison cached delegations in Recursor.

Risk And Classification

Primary CVSS: v3.1 8.2 HIGH from security@open-xchange.com

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

Problem Types: CWE-294 | Insufficient Verification of Data Authenticity

Version	Source	Type	Score	Severity	Vector
3.1	security@open-xchange.com	Secondary	8.2	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:L
3.1	CNA	CVSS	8.2	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:L

CVSS v3.1 Breakdown

Attack Vector
Network

Attack Complexity
Low

Privileges Required
None

User Interaction
None

Scope
Unchanged

Confidentiality
None

Integrity
High

Availability

Low

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Powerdns	Recursor	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	PowerDNS	Recursor	affected 5.3.0 5.3.1 semver	Not specified
CNA	PowerDNS	Recursor	affected 5.2.0 5.2.6 semver	Not specified
CNA	PowerDNS	Recursor	affected 5.1.0 5.1.8 semver	Not specified

References

Reference	Source	Link	Ta
docs.powerdns.com/recursor/security-advisories/powerdns-advisory-2025-06.html	security@open-xchange.com	docs.powerdns.com	Ve
CVE Program record	CVE.ORG	www.cve.org	ca
NVD vulnerability detail	NVD	nvd.nist.gov	ca

Vendor Comments And Credit

Discovery Credit

CNA: Yuxiao Wu from Tsinghua University (en)

CNA: Yunyi Zhang from Tsinghua University (en)

CNA: Baojun Liu from Tsinghua University (en)

CNA: Haixin Duan from Tsinghua University (en)

CNA: Shiming Liu from Network and Information Security Lab, Tsinghua University (en)

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

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