CVE-2006-4252

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

Summary

CVE	CVE-2006-4252
State	PUBLISHED
Assigner	debian
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-11-14 20:07:00 UTC
Updated	2026-04-23 00:35:47 UTC
Description	PowerDNS Recursor 3.1.3 and earlier allows remote attackers to cause a denial of service (resource exhaustion and applic

Risk And Classification

Primary CVSS: v2.0 5 from nvd@nist.gov

AV:N/AC:L/Au:N/C:N/I:N/A:P

Problem Types: NVD-CWE-Other | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

None

Availability

Partial

AV:N/AC:L/Au:N/C:N/I:N/A:P

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Powerdns	Recursor	2.0_rc1	All	All	All

Application	Powerdns	Recursor	2.8	All	All	All
Application	Powerdns	Recursor	2.9.15	All	All	All
Application	Powerdns	Recursor	2.9.16	All	All	All
Application	Powerdns	Recursor	2.9.17	All	All	All
Application	Powerdns	Recursor	2.9.18	All	All	All
Application	Powerdns	Recursor	3.0	All	All	All
Application	Powerdns	Recursor	3.0.1	All	All	All
Application	Powerdns	Recursor	3.1	All	All	All
Application	Powerdns	Recursor	3.1.1	All	All	All
Application	Powerdns	Recursor	3.1.2	All	All	All
Application	Powerdns	Recursor	All	All	All	All

Vendor Declared Affected Products

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

References

Reference
PowerDNS Remote Denial of Service and Buffer Overflow Vulnerabilities
PowerDNS Security Advisory 2006-02: Zero second CNAME TTLs can make PowerDNS exhaust allocated stack space, and crash
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
IBM X-Force Exchange
PowerDNS Recursor Two Vulnerabilities - Advisories - Secunia
SuSE Security announcements: [suse-security-announce] SUSE Security Announcement: powerdns denial of service (SUSE-SA:2006:070)
SUSE update for pdns - Advisories - Secunia
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

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