CVE-2002-2211

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

Summary

CVE	CVE-2002-2211
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2002-12-31 05:00:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	BIND 4 and BIND 8, when resolving recursive DNS queries for arbitrary hosts, allows remote attackers to conduct DNS cac

Risk And Classification

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

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

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

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

Partial

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Isc	Bind	4.9	All	All	All

Application	Isc	Bind	4.9.10	All	All	All
Application	Isc	Bind	4.9.2	All	All	All
Application	Isc	Bind	4.9.3	All	All	All
Application	Isc	Bind	4.9.4	All	All	All
Application	Isc	Bind	4.9.5	All	All	All
Application	Isc	Bind	4.9.5	p1	All	All
Application	Isc	Bind	4.9.6	All	All	All
Application	Isc	Bind	4.9.7	All	All	All
Application	Isc	Bind	4.9.8	All	All	All
Application	Isc	Bind	4.9.9	All	All	All
Application	Isc	Bind	8.2	All	All	All
Application	Isc	Bind	8.2.1	All	All	All
Application	Isc	Bind	8.2.2	All	All	All
Application	Isc	Bind	8.2.2	p1	All	All
Application	Isc	Bind	8.2.2	p2	All	All
Application	Isc	Bind	8.2.2	p3	All	All
Application	Isc	Bind	8.2.2	p4	All	All
Application	Isc	Bind	8.2.2	p5	All	All
Application	Isc	Bind	8.2.2	p6	All	All
Application	Isc	Bind	8.2.2	p7	All	All
Application	Isc	Bind	8.2.3	All	All	All
Application	Isc	Bind	8.2.4	All	All	All
Application	Isc	Bind	8.2.5	All	All	All
Application	Isc	Bind	8.2.6	All	All	All
Application	Isc	Bind	8.2.7	All	All	All
Application	Isc	Bind	8.3.0	All	All	All
Application	Isc	Bind	8.3.1	All	All	All
Application	Isc	Bind	8.3.2	All	All	All
Application	Isc	Bind	8.3.3	All	All	All
Application	Isc	Bind	8.3.4	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

Reference	Source	Link
A página não foi encontrada	af854a3a-2127-422b-91ae-364da2661108	www.rnp.br
CERT/CC Vulnerability Note VU#457875	af854a3a-2127-422b-91ae-364da2661108	www.kb.cert.org
MetaSolv Information for VU#457875	af854a3a-2127-422b-91ae-364da2661108	www.kb.cert.org
Security Update 2002-11-21 is available	af854a3a-2127-422b-91ae-364da2661108	lists.apple.com
SecurityFocus	af854a3a-2127-422b-91ae-364da2661108	www.securityfocus.c
Secunia - Advisories - HP-UX BIND4 DNS Cache Poisoning Vulnerability	af854a3a-2127-422b-91ae-364da2661108	secunia.com
ISC Information for VU#457875	af854a3a-2127-422b-91ae-364da2661108	www.kb.cert.org
Microsoft Corporation Information for VU#457875	af854a3a-2127-422b-91ae-364da2661108	www.kb.cert.org
Spiral Bound - The Most Informative Website About Internet Network	af854a3a-2127-422b-91ae-364da2661108	www.imconf.net
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-2127-422b-91ae-364da2661108	www.vupen.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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