CVE-2008-3630

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

Summary

CVE	CVE-2008-3630
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-09-11 01:13:09 UTC
Updated	2026-04-23 00:35:47 UTC
Description	mDNSResponder in Apple Bonjour for Windows before 1.0.5, when an application uses the Bonjour API for unicast DNS, d

Risk And Classification

Primary CVSS: v2.0 6.4 from nvd@nist.gov

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

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

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

Partial

Availability

Partial

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apple	Bonjour	1.0.4	unknown	windows	All

Operating System	Microsoft	Windows-nt	xp	sp3	All	All
Operating System	Microsoft	Windows 2000	-	All	All	All
Operating System	Microsoft	Windows 2003 Server	-	All	All	All
Operating System	Microsoft	Windows Vista	-	All	All	All
Operating System	Microsoft	Windows Xp	-	sp2	All	All

Vendor Declared Affected Products

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

References

Reference	Source
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-2127-
APPLE-SA-2009-09-09 Bonjour for Windows 1.0.5	af854a3a-2127-
About the security content of Bonjour for Windows 1.0.5	af854a3a-2127-
Apple Bonjour for Windows mDNSResponder Remote Forged DNS Response Vulnerability	af854a3a-2127-
Apple Bonjour for Windows mDNSResponder Vulnerabilities - Secunia Advisories - Vulnerability Intelligence - Secunia.com	af854a3a-2127-
Apple Bonjour for Windows DNS Query Port Entropy Weakness Lets Remote Users Spoof the System - SecurityTracker	af854a3a-2127-
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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