CVE-2004-0882

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

Summary

CVE	CVE-2004-0882
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2005-01-27 05:00:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	Buffer overflow in the QFILEPATHINFO request handler in Samba 3.0.x through 3.0.7 may allow remote attackers to execu

Risk And Classification

Primary CVSS: v2.0 10 from nvd@nist.gov

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

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

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Conectiva	Linux	10.0	All	All	All

Operating System	Redhat	Enterprise Linux	2.1	All	advanced_server	All
Operating System	Redhat	Enterprise Linux	2.1	All	advanced_server_ia64	All
Operating System	Redhat	Enterprise Linux	2.1	All	enterprise_server	All
Operating System	Redhat	Enterprise Linux	2.1	All	enterprise_server_ia64	All
Operating System	Redhat	Enterprise Linux	2.1	All	workstation	All
Operating System	Redhat	Enterprise Linux	2.1	All	workstation_ia64	All
Operating System	Redhat	Enterprise Linux	3.0	All	advanced_server	All
Operating System	Redhat	Enterprise Linux	3.0	All	enterprise_server	All
Operating System	Redhat	Enterprise Linux	3.0	All	workstation_server	All
Operating System	Redhat	Enterprise Linux Desktop	3.0	All	All	All
Operating System	Redhat	Fedora Core	core_2.0	All	All	All
Operating System	Redhat	Fedora Core	core_3.0	All	All	All
Operating System	Redhat	Linux Advanced Workstation	2.1	All	ia64	All
Operating System	Redhat	Linux Advanced Workstation	2.1	All	itanium_processor	All
Application	Samba	Samba	3.0.0	All	All	All
Application	Samba	Samba	3.0.1	All	All	All
Application	Samba	Samba	3.0.2	All	All	All
Application	Samba	Samba	3.0.2a	All	All	All
Application	Samba	Samba	3.0.3	All	All	All
Application	Samba	Samba	3.0.4	All	All	All
Application	Samba	Samba	3.0.4	rc1	All	All
Application	Samba	Samba	3.0.5	All	All	All
Application	Samba	Samba	3.0.6	All	All	All
Application	Samba	Samba	3.0.7	All	All	All
Operating System	Ubuntu	Ubuntu Linux	4.1	All	ia64	All
Operating System	Ubuntu	Ubuntu Linux	4.1	All	ppc	All

Vendor Declared Affected Products

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

References

Reference	Sourc
www.osvdb.org/11782	af854a
Secunia - Advisories - Samba QFILEPATHINFO Request Handler Buffer Overflow Vulnerability	af854a
P-038: Samba Vulnerabilities	af854a
Security Announcement	af854a

Security Announcement	af854a
US-CERT Vulnerability Note VU#457622	af854a
'[SAMBA] CAN-2004-0882: Possiebl Buffer Overrun in smbd' - MARC	af854a
SecurityTracker.com Archives - Samba QFILEPATHINFO Buffer Overflow Lets Remote Authenticated Users Execute Arbitrary Code	af854a
www.trustix.net/errata/2004/0058	af854a
'Advisory 13/2004: Samba 3.x QFILEPATHINFO unicode filename buffer overflow' - MARC	af854a
Repository / Oval Repository	af854a
Home - Conectiva	af854a
APPLE-SA-2005-03-21 Security Update 2005-003	af854a
e-matters : SECURITY	af854a
'[OpenPKG-SA-2004.054] OpenPKG Security Advisory (samba)' - MARC	af854a
IBM X-Force Exchange	af854a
ftp.sco.com/pub/updates/UnixWare/SCOSA-2005.17/SCOSA-2005.17.txt	af854a
patches.sgi.com/support/free/security/advisories/20041201-01-P	af854a
CVE Program record	CVE.C
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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