



CVE-2004-0686

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

Summary

CVE	CVE-2004-0686
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2004-07-27 04:00:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	Buffer overflow in Samba 2.2.x to 2.2.9, and 3.0.0 to 3.0.4, when the "mangling method = hash" option is enabled in smb.cc

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	Samba	Samba	All	All	All	All

Vendor Declared Affected Products				
Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified
References				
Reference				Source
'TSSA-2004-014 - samba' - MARC				af854a3a-2127-422b-9
Home - Conectiva				af854a3a-2127-422b-9
Security Announcement				af854a3a-2127-422b-9
'[security bulletin] SSRT4782 rev. 0 HP-UX CIFS Server potential remote root access' - MARC				af854a3a-2127-422b-9
Home - Conectiva				af854a3a-2127-422b-9
redhat.com Red Hat Support				af854a3a-2127-422b-9
'[FLSA-2004:2102] Updated samba packages fix security vulnerability [updated]' - MARC				af854a3a-2127-422b-9
Gentoo Linux Documentation -- Samba: Multiple buffer overflows				af854a3a-2127-422b-9
www.trustix.org/errata/2004/0039				af854a3a-2127-422b-9
www.mandrakesecure.net/en/advisories/advisory.php				af854a3a-2127-422b-9
#57664: Security Vulnerability in Samba May Allow Unauthorized Root Privileges java.lang.NullPointerException				af854a3a-2127-422b-9
Repository / Oval Repository				af854a3a-2127-422b-9
#101584: Security Vulnerabilities in Samba May Allow Unauthorized Root Privileges (formerly Document ID: 57664)				af854a3a-2127-422b-9
IBM X-Force Exchange				af854a3a-2127-422b-9
'[OpenPKG-SA-2004.033] OpenPKG Security Advisory (samba)' - MARC				af854a3a-2127-422b-9
'Security Release - Samba 3.0.5 and 2.2.10' - MARC				af854a3a-2127-422b-9
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.				

