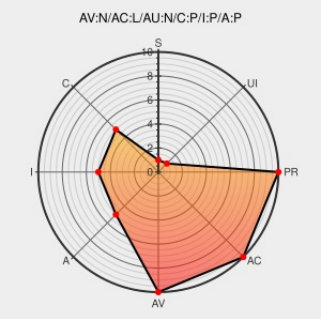
CVE-2004-0815

Published on: 10/16/2004 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:11 PM UTC

CVE-2004-0815

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Samba from Samba contain the following vulnerability:

The unix_clean_name function in Samba 2.2.x through 2.2.11, and 3.0.x before 3.0.2a, trims certain directory names down to absolute paths, which could allow remote attackers to bypass the specified share restrictions and read, write, or list arbitrary files via "/.////" style sequences in pathnames.

CVE-2004-0815 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 7.5 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
SecurityFocus	www.securityfocus.com text/html	BUGTRAQ 20041005 ERRATA: Potential Arbitrary File Access (CAN-2004-0815)
Debian -- Security Information -- DSA-600-1 samba	Patch Vendor Advisory www.debian.org Depreciated Link text/html	DEBIAN DSA-600
No Description Provided	bugzilla.fedora.us Inactive Link Not Archived	FEDORA FLSA:2102
No Description Provided	sunsolve.sun.com	SUNALERT 200529

	Inactive Link Not Archived	
No Description Provided	www.mandrakesecure.net Inactive Link Not Archived	MANDRAKE MDKSA-2004:104
'Samba Security Announcement -- Potential Arbitrary File Access' - MARC	marc.info text/html	BUGTRAQ 20040930 Samba Security Announcement -- Potential Arbitrary File Access
Home - Conectiva	Patch Vendor Advisory distro.conectiva.com.br text/html	CONECTIVA CLA-2004:873
	www.trustix.org text/plain Inactive Link Not Archived	TRUSTIX 2004-0051
Support	www.redhat.com text/html	REDHAT RHSA-2004:498
Accenture | Let there be change	Exploit Vendor Advisory www.idefense.com text/html	IDEFENSE 20040930 Samba Arbitrary File Access Vulnerability
Security Announcement	web.archive.org text/html Inactive Link Not Archived	SUSE SUSE-SA:2004:035
#101584: Security Vulnerabilities in Samba May Allow Unauthorized Root Privileges (formerly Document ID: 57664)	web.archive.org text/html Inactive Link Not Archived	SUNALERT 101584
news.samba.org	us4.samba.org text/html	CONFIRM us4.samba.org/samba/news/#security_2.2.12
#57664: Security Vulnerability in Samba May Allow Unauthorized Root Privileges java.lang.NullPointerException	web.archive.org text/html Inactive Link Not Archived	SUNALERT 57664
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF samba-file-access(17556)
Samba Remote Arbitrary File Access Vulnerability	Patch Vendor Advisory cve.report (archive) text/html	BID 11281

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Samba	Samba	2.2.0	All	All	All
Application	Samba	Samba	2.2.0a	All	All	All

Application	Samba	Samba	2.2.11	All	All	All
Application	Samba	Samba	2.2.1a	All	All	All
Application	Samba	Samba	2.2.2	All	All	All
Application	Samba	Samba	2.2.3	All	All	All
Application	Samba	Samba	2.2.3a	All	All	All
Application	Samba	Samba	2.2.4	All	All	All
Application	Samba	Samba	2.2.5	All	All	All
Application	Samba	Samba	2.2.6	All	All	All
Application	Samba	Samba	2.2.7	All	All	All
Application	Samba	Samba	2.2.7a	All	All	All
Application	Samba	Samba	2.2.8	All	All	All
Application	Samba	Samba	2.2.8a	All	All	All
Application	Samba	Samba	2.2.9	All	All	All
Application	Samba	Samba	2.2a	All	All	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	2.2.0	All	All	All
Application	Samba	Samba	2.2.0a	All	All	All
Application	Samba	Samba	2.2.11	All	All	All
Application	Samba	Samba	2.2.1a	All	All	All
Application	Samba	Samba	2.2.2	All	All	All
Application	Samba	Samba	2.2.3	All	All	All
Application	Samba	Samba	2.2.3a	All	All	All
Application	Samba	Samba	2.2.4	All	All	All
Application	Samba	Samba	2.2.5	All	All	All
Application	Samba	Samba	2.2.6	All	All	All
Application	Samba	Samba	2.2.7	All	All	All
Application	Samba	Samba	2.2.7a	All	All	All
Application	Samba	Samba	2.2.8	All	All	All
Application	Samba	Samba	2.2.8a	All	All	All
Application	Samba	Samba	2.2.9	All	All	All
Application	Samba	Samba	2.2a	All	All	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

- cpe:2.3:a:samba:samba:2.2.0:*:*:*:*:*:*:*:
- cpe:2.3:a:samba:samba:2.2.0a:*:*:*:*:*:*:*:
- cpe:2.3:a:samba:samba:2.2.11:*:*:*:*:*:*:*:
- cpe:2.3:a:samba:samba:2.2.1a:*:*:*:*:*:*:*:
- cpe:2.3:a:samba:samba:2.2.2:*:*:*:*:*:*:*:
- cpe:2.3:a:samba:samba:2.2.3:*:*:*:*:*:*:*:
- cpe:2.3:a:samba:samba:2.2.3a:*:*:*:*:*:*:*:
- cpe:2.3:a:samba:samba:2.2.4:*:*:*:*:*:*:*:
- cpe:2.3:a:samba:samba:2.2.5:*:*:*:*:*:*:*:
- cpe:2.3:a:samba:samba:2.2.6:*:*:*:*:*:*:*:
- cpe:2.3:a:samba:samba:2.2.7:*:*:*:*:*:*:*:
- cpe:2.3:a:samba:samba:2.2.7a:*:*:*:*:*:*:*:
- cpe:2.3:a:samba:samba:2.2.8:*:*:*:*:*:*:*:
- cpe:2.3:a:samba:samba:2.2.8a:*:*:*:*:*:*:*:
- cpe:2.3:a:samba:samba:2.2.9:*:*:*:*:*:*:*:
- cpe:2.3:a:samba:samba:2.2a:*:*:*:*:*:*:*:
- cpe:2.3:a:samba:samba:3.0.0:*:*:*:*:*:*:*:
- cpe:2.3:a:samba:samba:3.0.1:*:*:*:*:*:*:*:
- cpe:2.3:a:samba:samba:3.0.2:*:*:*:*:*:*:*:
- cpe:2.3:a:samba:samba:3.0.2a:*:*:*:*:*:*:*:
- cpe:2.3:a:samba:samba:2.2.0:*:*:*:*:*:*:*:
- cpe:2.3:a:samba:samba:2.2.0a:*:*:*:*:*:*:*:
- cpe:2.3:a:samba:samba:2.2.11:*:*:*:*:*:*:*:
- cpe:2.3:a:samba:samba:2.2.1a:*:*:*:*:*:*:*:
- cpe:2.3:a:samba:samba:2.2.2:*:*:*:*:*:*:*:
- cpe:2.3:a:samba:samba:2.2.3:*:*:*:*:*:*:*:

cpe:2.3:a:samba:samba:2.2.3a:*:*:*:*:*:*:*:

cpe:2.3:a:samba:samba:2.2.4:*:*:*:*:*:*:*:

cpe:2.3:a:samba:samba:2.2.5:*:*:*:*:*:*:*:

cpe:2.3:a:samba:samba:2.2.6:*:*:*:*:*:*:*:

cpe:2.3:a:samba:samba:2.2.7:*:*:*:*:*:*:*:

cpe:2.3:a:samba:samba:2.2.7a:*:*:*:*:*:*:*:

cpe:2.3:a:samba:samba:2.2.8:*:*:*:*:*:*:*:

cpe:2.3:a:samba:samba:2.2.8a:*:*:*:*:*:*:*:

cpe:2.3:a:samba:samba:2.2.9:*:*:*:*:*:*:*:

cpe:2.3:a:samba:samba:2.2a:*:*:*:*:*:*:*:

cpe:2.3:a:samba:samba:3.0.0:*:*:*:*:*:*:*:

cpe:2.3:a:samba:samba:3.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:samba:samba:3.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:samba:samba:3.0.2a:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→