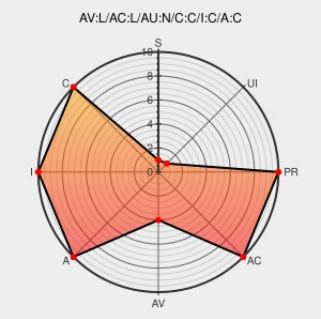
CVE-2003-1528

Published on: 12/31/2003 05:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:43 PM UTC

CVE-2003-1528

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



Certain versions of Siemens Networker from Fujitsu contain the following vulnerability:

nsr_shutdown in Fujitsu Siemens NetWorker 6.0 allows local users to overwrite arbitrary files via a symlink attack on the nsrsh[PID] temporary file.

CVE-2003-1528 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 7.2 - HIGH

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Networker 6.0 - possible symlink attack - CXSecurity.com	Exploit, securityreason.com, text/html	SREASON 3353
SecurityFocus	www.securityfocus.com, text/html	BUGTRAQ 20040119 Networker 6.0 - possible symlink attack
NetWorker 'nsr_shutdown' Unsafe Temporary File May Let Local Users Gain Root Privileges - SecurityTracker	www.securitytracker.com, text/html	SECTRACK 1008801
Legato NetWorker NSR_Shutdown Script Temporary File Symlink Attack Vulnerability	cve.report (archive), text/html	BID 9446

comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Fujitsu	Siemens Networker	6.0	All	All	All
Application	Fujitsu	Siemens Networker	6.0	All	All	All

cpe:2.3:a:fujitsu:siemens_networker:6.0:*:*:*:*:*:*:*:

cpe:2.3:a:fujitsu:siemens_networker:6.0:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→