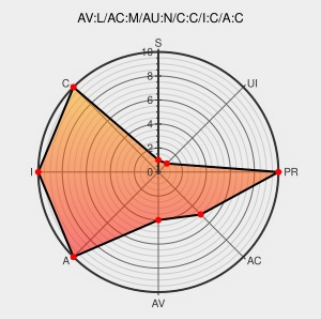
CVE-2010-2020

Published on: 05/28/2010 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:09 PM UTC

CVE-2010-2020

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



Certain versions of Freebsd from Freebsd contain the following vulnerability:

sys/nfsclient/nfs_vfsops.c in the NFS client in the kernel in FreeBSD 7.2 through 8.1-PRERELEASE, when vfs.usermount is enabled, does not validate the length of a certain fhsize parameter, which allows local users to gain privileges via a crafted mount request.

CVE-2010-2020 has been assigned by secteam@freebsd.org to track the vulnerability

CVSS2 Score: 6.9 - MEDIUM

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

CVE References

Description	Tags	Link
	Vendor Advisory, security.FreeBSD.org, text/plain	FREEBSD FreeBSD-SA-10:06
FreeBSD Kernel mountnfs() Exploit	www.exploit-db.com, Proof of Concept, text/x-c	EXPLOIT-DB 14003
FreeBSD Kernel nfs_mount() Exploit	www.exploit-db.com, Proof of Concept, text/html	EXPLOIT-DB 14002
SecurityTracker.com Archives - FreeBSD Parameter Validation Flaw in nfsclient Lets Local Users Gain Elevated Privileges	securitytracker.com, text/html	SECTRACK 1024039

are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to 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
Operating System	Freebsd	Freebsd	7.2	All	All	All
Operating System	Freebsd	Freebsd	7.2	pre-release	All	All
Operating System	Freebsd	Freebsd	7.2	stable	All	All
Operating System	Freebsd	Freebsd	8.0	All	All	All
Operating System	Freebsd	Freebsd	8.1-prerelease	All	All	All
Operating System	Freebsd	Freebsd	7.2	All	All	All
Operating System	Freebsd	Freebsd	7.2	pre-release	All	All
Operating System	Freebsd	Freebsd	7.2	stable	All	All
Operating System	Freebsd	Freebsd	8.0	All	All	All
Operating System	Freebsd	Freebsd	8.1-prerelease	All	All	All

cpe:2.3:o:freebsd:freebsd:7.2:*:*:*:*:*:*:*:

cpe:2.3:o:freebsd:freebsd:7.2:pre-release:*:*:*:*:*:*:*:

cpe:2.3:o:freebsd:freebsd:7.2:stable:*:*:*:*:*:*:*:

cpe:2.3:o:freebsd:freebsd:8.0:*:*:*:*:*:*:*:

cpe:2.3:o:freebsd:freebsd:8.1-prerelease:*:*:*:*:*:*:*:

cpe:2.3:o:freebsd:freebsd:7.2:*:*:*:*:*:*:*:

cpe:2.3:o:freebsd:freebsd:7.2:pre-release:*:*:*:*:*:*:*:

cpe:2.3:o:freebsd:freebsd:7.2:stable:*:*:*:*:*:*:*:

cpe:2.3:o:freebsd:freebsd:8.0:*:*:*:*:*:*:*:

cpe:2.3:o:freebsd:freebsd:8.1-prerelease:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→