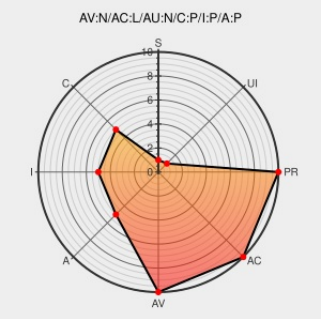
CVE-2013-3266

Published on: 05/02/2013 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:30 PM UTC

CVE-2013-3266

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



Certain versions of Freebsd from Freebsd contain the following vulnerability:

The nfsrvd_readdir function in sys/fs/nfsserver/nfs_nfsdport.c in the new NFS server in FreeBSD 8.0 through 9.1-RELEASE-p3 does not verify that a READDIR request is for a directory node, which allows remote attackers to cause a denial of service (memory corruption) or possibly execute arbitrary code by specifying a plain file instead of a directory.

CVE-2013-3266 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
Security Advisory SA53241 - FreeBSD NFS Server READDIR Request Processing Security Issue - Secunia	web.archive.org, text/html	SECUNIA 53241
	Patch, Vendor Advisory, www.freebsd.org, text/plain	FREEBSD FreeBSD-SA-13:05
Debian -- Security Information -- DSA-2672-1 kfreebsd-9	www.debian.org, Depreciated Link, text/html	DEBIAN DSA-2672
FreeBSD NFS Server Input Validation Bug May Let Remote Users Execute Arbitrary Code - SecurityTracker	www.securitytracker.com, text/html	SECTRACK 1028491

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that 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	8.0	All	All	All
Operating System	Freebsd	Freebsd	8.1	All	All	All
Operating System	Freebsd	Freebsd	8.2	All	All	All
Operating System	Freebsd	Freebsd	8.3	All	All	All
Operating System	Freebsd	Freebsd	9.0	All	All	All
Operating System	Freebsd	Freebsd	9.1	All	All	All
Operating System	Freebsd	Freebsd	8.0	All	All	All
Operating System	Freebsd	Freebsd	8.1	All	All	All
Operating System	Freebsd	Freebsd	8.2	All	All	All
Operating System	Freebsd	Freebsd	8.3	All	All	All
Operating System	Freebsd	Freebsd	9.0	All	All	All
Operating System	Freebsd	Freebsd	9.1	All	All	All

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

cpe:2.3:o:freebsd:freebsd:8.1:*:*:*:*:*:*:*:

cpe:2.3:o:freebsd:freebsd:8.2:*:*:*:*:*:*:*:

cpe:2.3:o:freebsd:freebsd:8.3:*:*:*:*:*:*:*:

cpe:2.3:o:freebsd:freebsd:9.0:*:*:*:*:*:*:*:

cpe:2.3:o:freebsd:freebsd:9.1:*:*:*:*:*:*:*:

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

cpe:2.3:o:freebsd:freebsd:8.1:*:*:*:*:*:*:*

cpe:2.3:o:freebsd:freebsd:8.2:*:*:*:*:*:*:*

cpe:2.3:o:freebsd:freebsd:8.3:*:*:*:*:*:*:*

cpe:2.3:o:freebsd:freebsd:9.0:*:*:*:*:*:*:*

cpe:2.3:o:freebsd:freebsd:9.1:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→