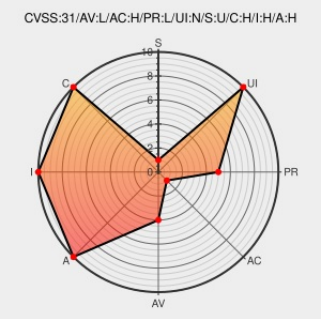
CVE-2020-7460

Published on: 08/06/2020 12:00:00 AM UTC

Last Modified on: 07/01/2022 06:44:00 PM UTC

CVE-2020-7460

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



Certain versions of Freebsd from Freebsd contain the following vulnerability:

In FreeBSD 12.1-STABLE before r363918, 12.1-RELEASE before p8, 11.4-STABLE before r363919, 11.4-RELEASE before p2, and 11.3-RELEASE before p12, the sendmsg system call in the compat32 subsystem on 64-bit platforms has a time-of-check to time-of-use vulnerability allowing a mailcious userspace program to modify control message headers after they were validation.

CVE-2020-7460 has been assigned by secteam@freebsd.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	HIGH	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 4.4 - MEDIUM

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

CVE References

Description	Tags	Link
August 2020 FreeBSD Vulnerabilities in NetApp Products | NetApp Product Security	security.netapp.com text/html	CONFIRM security.netapp.com/advisory/ntap-20200821-

		0005/
ZDI-20-949 | Zero Day Initiative	Third Party Advisory VDB Entry www.zerodayinitiative.com text/html	MISC www.zerodayinitiative.com/advisories/ZDI-20-949/
	Vendor Advisory security.FreeBSD.org text/plain	MISC security.FreeBSD.org/advisories/FreeBSD-SA-20:23.sendmsg.asc

Related QID Numbers

690467 Free Berkeley Software Distribution (FreeBSD) Security Update for Free Berkeley Software Distribution (FreeBSD) (8db74c04-d794-11ea-88f8-901b0ef719ab)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Freebsd	Freebsd	11.3	-	All	All
Operating System	Freebsd	Freebsd	11.3	p1	All	All
Operating System	Freebsd	Freebsd	11.3	p10	All	All
Operating System	Freebsd	Freebsd	11.3	p11	All	All
Operating System	Freebsd	Freebsd	11.3	p2	All	All
Operating System	Freebsd	Freebsd	11.3	p3	All	All
Operating System	Freebsd	Freebsd	11.3	p4	All	All
Operating System	Freebsd	Freebsd	11.3	p5	All	All
Operating System	Freebsd	Freebsd	11.3	p6	All	All
Operating System	Freebsd	Freebsd	11.3	p7	All	All
Operating System	Freebsd	Freebsd	11.3	p8	All	All
Operating System	Freebsd	Freebsd	11.3	p9	All	All
Operating System	Freebsd	Freebsd	11.4	-	All	All
Operating	Freebsd	Freebsd	11.4	p1	All	All

System						
Operating System	Freebsd	Freebsd	12.1	-	All	All
Operating System	Freebsd	Freebsd	12.1	p1	All	All
Operating System	Freebsd	Freebsd	12.1	p2	All	All
Operating System	Freebsd	Freebsd	12.1	p3	All	All
Operating System	Freebsd	Freebsd	12.1	p4	All	All
Operating System	Freebsd	Freebsd	12.1	p6	All	All
Operating System	Freebsd	Freebsd	12.1	p7	All	All
Operating System	Freebsd	Freebsd	11.3	-	All	All
Operating System	Freebsd	Freebsd	11.3	p1	All	All
Operating System	Freebsd	Freebsd	11.3	p10	All	All
Operating System	Freebsd	Freebsd	11.3	p11	All	All
Operating System	Freebsd	Freebsd	11.3	p2	All	All
Operating System	Freebsd	Freebsd	11.3	p3	All	All
Operating System	Freebsd	Freebsd	11.3	p4	All	All
Operating System	Freebsd	Freebsd	11.3	p5	All	All
Operating System	Freebsd	Freebsd	11.3	p6	All	All
Operating System	Freebsd	Freebsd	11.3	p7	All	All
Operating System	Freebsd	Freebsd	11.3	p8	All	All
Operating System	Freebsd	Freebsd	11.3	p9	All	All
Operating System	Freebsd	Freebsd	11.4	-	All	All
Operating System	Freebsd	Freebsd	11.4	p1	All	All
Operating System	Freebsd	Freebsd	12.1	-	All	All
Operating	Freebsd	Freebsd	12.1	p1	All	All

Operating System	Freebsd	Freebsd	12.1	p1	All	All
Operating System	Freebsd	Freebsd	12.1	p2	All	All
Operating System	Freebsd	Freebsd	12.1	p3	All	All
Operating System	Freebsd	Freebsd	12.1	p4	All	All
Operating System	Freebsd	Freebsd	12.1	p6	All	All
Operating System	Freebsd	Freebsd	12.1	p7	All	All

cpe:2.3:o:freebsd:freebsd:11.3:-:*:*:*:*:*:*:

cpe:2.3:o:freebsd:freebsd:11.3:p1:*:*:*:*:*:*:

cpe:2.3:o:freebsd:freebsd:11.3:p10:*:*:*:*:*:*:

cpe:2.3:o:freebsd:freebsd:11.3:p11:*:*:*:*:*:*:

cpe:2.3:o:freebsd:freebsd:11.3:p2:*:*:*:*:*:*:

cpe:2.3:o:freebsd:freebsd:11.3:p3:*:*:*:*:*:*:

cpe:2.3:o:freebsd:freebsd:11.3:p4:*:*:*:*:*:*:

cpe:2.3:o:freebsd:freebsd:11.3:p5:*:*:*:*:*:*:

cpe:2.3:o:freebsd:freebsd:11.3:p6:*:*:*:*:*:*:

cpe:2.3:o:freebsd:freebsd:11.3:p7:*:*:*:*:*:*:

cpe:2.3:o:freebsd:freebsd:11.3:p8:*:*:*:*:*:*:

cpe:2.3:o:freebsd:freebsd:11.3:p9:*:*:*:*:*:*:

cpe:2.3:o:freebsd:freebsd:11.4:-:*:*:*:*:*:*:

cpe:2.3:o:freebsd:freebsd:11.4:p1:*:*:*:*:*:*:

cpe:2.3:o:freebsd:freebsd:12.1:-:*:*:*:*:*:*:

cpe:2.3:o:freebsd:freebsd:12.1:p1:*:*:*:*:*:*:

cpe:2.3:o:freebsd:freebsd:12.1:p2:*:*:*:*:*:*:

cpe:2.3:o:freebsd:freebsd:12.1:p3:*:*:*:*:*:*:

cpe:2.3:o:freebsd:freebsd:12.1:p4:*:*:*:*:*:*:

cpe:2.3:o:freebsd:freebsd:12.1:p6:*:*:*:*:*:*:

cpe:2.3:o:freebsd:freebsd:12.1:p7:*:*:*:*:*:*:

cpe:2.3:o:freebsd:freebsd:11.3:-:*:*:*:*:*:*:

cpe:2.3:o:freebsd:freebsd:11.3:p1:*:*:*:*:*:*:

cpe:2.3:o:freebsd:freebsd:11.3:p10:*:*:*:*:*:*:

cpe:2.3:o:freebsd:freebsd:11.3:p11:*:*:*:*:*:*:

cpe:2.3:o:freebsd:freebsd:11.3:p2:*:*:*:*:*:*:

cpe:2.3:o:freebsd:freebsd:11.3:p3:*:*:*:*:*:*:

cpe:2.3:o:freebsd:freebsd:11.3:p4:*:*:*:*:*:*:

cpe:2.3:o:freebsd:freebsd:11.3:p5:*:*:*:*:*:*:

cpe:2.3:o:freebsd:freebsd:11.3:p6:*:*:*:*:*:*:

cpe:2.3:o:freebsd:freebsd:11.3:p7:*:*:*:*:*:*:

cpe:2.3:o:freebsd:freebsd:11.3:p8:*:*:*:*:*:*:

cpe:2.3:o:freebsd:freebsd:11.3:p9:*:*:*:*:*:*:

cpe:2.3:o:freebsd:freebsd:11.4:-:*:*:*:*:*:*:

cpe:2.3:o:freebsd:freebsd:11.4:p1:*:*:*:*:*:*:

cpe:2.3:o:freebsd:freebsd:12.1:-:*:*:*:*:*:*:

cpe:2.3:o:freebsd:freebsd:12.1:p1:*:*:*:*:*:*:

cpe:2.3:o:freebsd:freebsd:12.1:p2:*:*:*:*:*:*:

cpe:2.3:o:freebsd:freebsd:12.1:p3:*:*:*:*:*:*:

cpe:2.3:o:freebsd:freebsd:12.1:p4:*:*:*:*:*:*:

cpe:2.3:o:freebsd:freebsd:12.1:p6:*:*:*:*:*:*:

cpe:2.3:o:freebsd:freebsd:12.1:p7:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@LinInfoSec	Freebsd - CVE-2020-7460: security.FreeBSD.org/advisories/Fre…	2022-07-01 22:00:44

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report