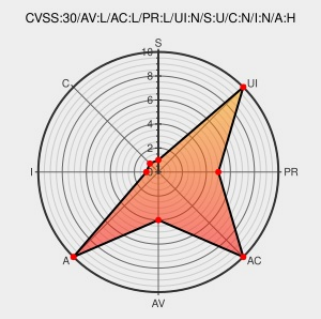
CVE-2018-6925

Published on: 09/28/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:46 PM UTC

CVE-2018-6925

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



Certain versions of Freebsd from Freebsd contain the following vulnerability:

In FreeBSD before 11.2-STABLE(r338986), 11.2-RELEASE-p4, 11.1-RELEASE-p15, 10.4-STABLE(r338985), and 10.4-RELEASE-p13, due to improper maintenance of IPv6 protocol control block flags through various failure paths, an unprivileged authenticated local user may be able to cause a NULL pointer dereference causing the kernel to crash.

CVE-2018-6925 has been assigned by secteam@freebsd.org to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **FreeBSD** - **FreeBSD** version **11.2 before 11.2-RELEASE-p4**

Affected Vendor/Software: **FreeBSD** - **FreeBSD** version **11.1 before 11.1-RELEASE-p15**

Affected Vendor/Software: **FreeBSD** - **FreeBSD** version **10.x before 10.4-RELEASE-p13**

CVSS3 Score: 5.5 - MEDIUM

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

CVSS2 Score: 4.9 - MEDIUM

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

CVE References

Description	Tags	Link
Secunia Advisories	www.flexera.com text/html	MISC www.flexera.com/company/secunia-research/advisories/SR-2018-21.html
	Patch Vendor Advisory security.FreeBSD.org text/plain	CONFIRM security.FreeBSD.org/advisories/FreeBSD-EN-18:11.listen.asc

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	All	All	All	All
Operating System	Freebsd	Freebsd	10.4	All	All	All
Operating System	Freebsd	Freebsd	10.4	p13	All	All
Operating System	Freebsd	Freebsd	11.1	p15	All	All
Operating System	Freebsd	Freebsd	11.2	p4	All	All
Operating System	Freebsd	Freebsd	All	All	All	All
Operating System	Freebsd	Freebsd	10.4	All	All	All
Operating System	Freebsd	Freebsd	10.4	p13	All	All
Operating System	Freebsd	Freebsd	11.1	p15	All	All
Operating System	Freebsd	Freebsd	11.2	p4	All	All

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

cpe:2.3:o:freebsd:freebsd:10.4:*:*:*:*:*:*:*:

cpe:2.3:o:freebsd:freebsd:10.4:p13:*:*:*:*:*:*:

cpe:2.3:o:freebsd:freebsd:11.1:p15:*:*:*:*:*:*:

cpe:2.3:o:freebsd:freebsd:11.2:p4:*:*:*:*:*:*:

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

cpe:2.3:o:freebsd:freebsd:10.4:*:*:*:*:*:*:*:

cpe:2.3:o:freebsd:freebsd:10.4:p13:*:*:*:*:*:*:

cpe:2.3:o:freebsd:freebsd:11.1:p15:*:*:*:*:*:*:

cpe:2.3:o:freebsd:freebsd:11.2:p4:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
/r/Juniper	EX Series JUNOS Software Release Notification 12.3R12-S19 and 15.1R7-S10	2021-09-06 06:57:35

← Previous ID

Next ID→