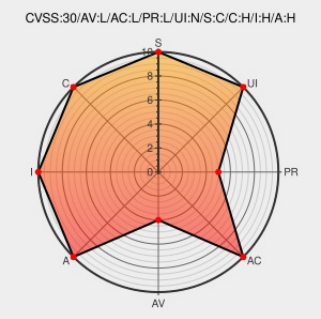
CVE-2019-5596

Published on: 02/12/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:59 PM UTC

CVE-2019-5596

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



Certain versions of Freebsd from Freebsd contain the following vulnerability:

In FreeBSD 11.2-STABLE after r338618 and before r343786, 12.0-STABLE before r343781, and 12.0-RELEASE before 12.0-RELEASE-p3, a bug in the reference count implementation for UNIX domain sockets can cause a file structure to be incorrectly released potentially allowing a malicious local user to gain root privileges or escape from a jail.

CVE-2019-5596 has been assigned by secteam@freebsd.org to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **FreeBSD** - **FreeBSD** version **FreeBSD 12.0 before 12.0-RELEASE-p3**

CVSS3 Score: 8.8 - HIGH

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

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

FreeBSD fd Privilege Escalation ≈ Packet Storm	packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/155790/FreeBSD-fd-Privilege-Escalation.html
	Patch Third Party Advisory security.FreeBSD.org text/plain	FREEBSD FreeBSD-SA-19:02

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
Application	Freebsd	Freebsd	11.2	All	All	All
Application	Freebsd	Freebsd	12.0	All	All	All
Application	Freebsd	Freebsd	11.2	All	All	All
Application	Freebsd	Freebsd	12.0	All	All	All

cpe:2.3:a:freebsd:freebsd:11.2:*:*:*:*:*:*:*:

cpe:2.3:a:freebsd:freebsd:12.0:*:*:*:*:*:*:*:

cpe:2.3:a:freebsd:freebsd:11.2:*:*:*:*:*:*:*:

cpe:2.3:a:freebsd:freebsd:12.0:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→