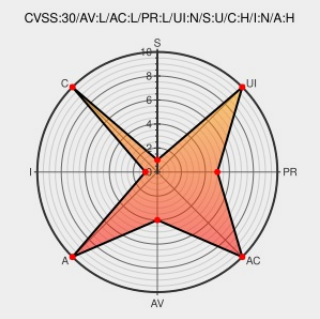
CVE-2018-6924

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

Last Modified on: 03/23/2021 11:24:47 PM UTC

CVE-2018-6924

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



Certain versions of Freebsd from Freebsd contain the following vulnerability:

In FreeBSD before 11.1-STABLE, 11.2-RELEASE-p3, 11.1-RELEASE-p14, 10.4-STABLE, and 10.4-RELEASE-p12, insufficient validation in the ELF header parser could allow a malicious ELF binary to cause a kernel crash or disclose kernel memory.

CVE-2018-6924 has been assigned by secteam@freebsd.org to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **FreeBSD** - **FreeBSD** version **before 11.1-STABLE, 11.2-RELEASE-p3, 11.1-RELEASE-p14, 10.4-STABLE, and 10.4-RELEASE-p12**

CVSS3 Score: 7.1 - HIGH

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

CVSS2 Score: 5.6 - MEDIUM

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

CVE References

Description	Tags	Link
FreeBSD Kernel ELF Header Parsing Error Lets Local Users Obtain Memory Contents and Cause the Target System to Crash - SecurityTracker	Third Party Advisory VDB Entry	SECTRACK

	www.securitytracker.com text/html	1041646
	Patch Vendor Advisory security.freebsd.org text/plain	FREEBSD FreeBSD-SA-18:12

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	11.2	All	All	All
Operating System	Freebsd	Freebsd	All	All	All	All
Operating System	Freebsd	Freebsd	10.4	All	All	All
Operating System	Freebsd	Freebsd	11.2	All	All	All

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

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

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

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

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

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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