

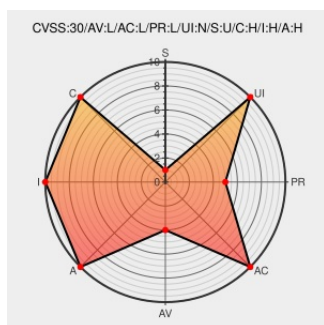


CVE-2017-1085

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

Last Modified on: 03/23/2021 11:26:37 PM UTC

CVE-2017-1085

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Freebsd](#) from [Freebsd](#) contain the following vulnerability:

In FreeBSD before 11.2-RELEASE, an application which calls `setrlimit()` to increase `RLIMIT_STACK` may turn a read-only memory region below the stack into a read-write region. A specially crafted executable could be exploited to execute arbitrary code in the user context.

CVE-2017-1085 has been assigned by secteam@freebsd.org to track the vulnerability - currently rated as **HIGH** severity.

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

CVSS3 Score: **7.8 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	LOW	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	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 - 'setrlimit' Stack Clash (PoC) - FreeBSD_x86	Third Party Advisory	EXPLOIT-DB 42279

dos Exploit

VDB Entry

www.exploit-db.com

Proof of Concept

text/html

Exploit

Technical Description

Third Party Advisory

www.qualys.com

text/plain

 MISC www.qualys.com/2017/06/19/stack-clash/stack-clash.txt

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→