



CVE-2019-15880

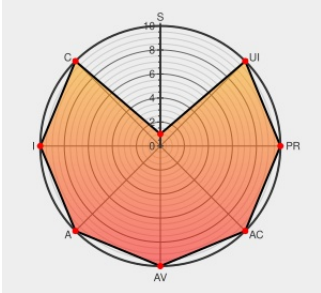
Published on: 05/13/2020 12:00:00 AM UTC

Last Modified on: 04/26/2022 07:54:00 PM UTC

CVE-2019-15880

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

CVSS:31/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H



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

In FreeBSD 12.1-STABLE before r356911, and 12.1-RELEASE before p5, insufficient checking in the cryptodev module allocated the size of a kernel buffer based on a user-supplied length allowing an unprivileged process to trigger a kernel panic.

CVE-2019-15880 has been assigned by secteam@freebsd.org to track the vulnerability - currently rated as **CRITICAL** severity.

CVSS3 Score: **9.8 - CRITICAL**

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

CVSS2 Score: **7.5 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
CVE-2019-15880 FreeBSD Vulnerability in NetApp Products NetApp Product Security	security.netapp.com text/html	CONFIRM security.netapp.com/advisory/ntap-20200518-0008/
	Vendor Advisory security.FreeBSD.org	MISC security.FreeBSD.org/advisories/FreeBSD-SA-

There are currently no QIDs associated with this CVE

Type	Vendor	Product	Version	Update	Edition	Language
------	--------	---------	---------	--------	---------	----------

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	-	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
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:-:*:*:*:*:*:						
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:*:*:*:*:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)

© [CVE.report](#) 2023  |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)