



CVE-2019-5599

Published on: 07/02/2019 12:00:00 AM UTC

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

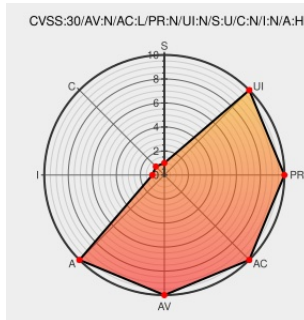
CVE-2019-5599

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



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

In FreeBSD 12.0-STABLE before r349197 and 12.0-RELEASE before 12.0-RELEASE-p6, a bug in the non-default RACK TCP stack can allow an attacker to cause several linked lists to grow unbounded and cause an expensive list traversal on every packet being processed, leading to resource exhaustion and a denial of service.

CVE-2019-5599 has been assigned by secteam@freebsd.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.5 - HIGH**

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

CVSS2 Score: **7.8 - HIGH**

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

CVE References

Description	Tags	Link
oss-security - Linux and FreeBSD Kernel: Multiple TCP-based remote denial of service issues	Mailing List Third Party Advisory www.openwall.com	MLIST [oss-security] 20190617 Linux and FreeBSD Kernel: Multiple TCP-based remote denial of service issues

	text/html	
No Description Provided	Third Party Advisory support.f5.com text/html	MISC support.f5.com/csp/article/K75521003
Public KB - SA44193 - 2019-06: Out-of-Cycle Advisory: Multiple Linux Kernel and FreeBSD vulnerabilities	Third Party Advisory kb.pulsesecure.net text/html	MISC kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44193
FreeBSD Security Advisory - FreeBSD-SA-19:08.rack ≈ Packet Storm	Third Party Advisory VDB Entry packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/153378/FreeBSD-Security-Advisory-FreeBSD-SA-19-08.rack.html
	Mitigation Vendor Advisory security.FreeBSD.org text/plain	FREEBSD FreeBSD-SA-19:08
Bugtraq: FreeBSD Security Advisory FreeBSD-SA-19:08.rack	Mailing List Mitigation Patch Third Party Advisory seclists.org text/html	BUGTRAQ 20190624 FreeBSD Security Advisory FreeBSD-SA-19:08.rack
CVE-2019-5599 FreeBSD TCP SACK Vulnerability in NetApp Products NetApp Product Security	Third Party Advisory security.netapp.com text/html	MISC security.netapp.com/advisory/ntap-20190625-0004/
Linux / FreeBSD TCP-Based Denial Of Service ≈ Packet Storm	Third Party Advisory VDB Entry packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/153329/Linux-FreeBSD-TCP-Based-Denial-Of-Service.html
VU#905115 - Multiple TCP Selective Acknowledgement (SACK) and Maximum Segment Size (MSS) networking vulnerabilities may cause denial-of-service conditions in Linux and FreeBSD kernels	Third Party Advisory US Government Resource www.kb.cert.org text/html	CERT-VN VU#905115
security-bulletins/2019-001.md at master · Netflix/security-bulletins · GitHub	Mitigation Third Party Advisory github.com text/html	MISC github.com/Netflix/security-bulletins/blob/master/advisories/third-party/2019-001.md

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	12.0	-	All	All
Operating System	Freebsd	Freebsd	12.0	p1	All	All

Operating System	Freebsd	Freebsd	12.0	p2	All	All
Operating System	Freebsd	Freebsd	12.0	p3	All	All
Operating System	Freebsd	Freebsd	12.0	p4	All	All
Operating System	Freebsd	Freebsd	12.0	p5	All	All
Operating System	Freebsd	Freebsd	12.0	-	All	All
Operating System	Freebsd	Freebsd	12.0	p1	All	All
Operating System	Freebsd	Freebsd	12.0	p2	All	All
Operating System	Freebsd	Freebsd	12.0	p3	All	All
Operating System	Freebsd	Freebsd	12.0	p4	All	All
Operating System	Freebsd	Freebsd	12.0	p5	All	All
cpe:2.3:o:freebsd:freebsd:12.0:-:*:*:*:*:*:						
cpe:2.3:o:freebsd:freebsd:12.0:p1:*:*:*:*:*:						
cpe:2.3:o:freebsd:freebsd:12.0:p2:*:*:*:*:*:						
cpe:2.3:o:freebsd:freebsd:12.0:p3:*:*:*:*:*:						
cpe:2.3:o:freebsd:freebsd:12.0:p4:*:*:*:*:*:						
cpe:2.3:o:freebsd:freebsd:12.0:p5:*:*:*:*:*:						
cpe:2.3:o:freebsd:freebsd:12.0:-:*:*:*:*:*:						
cpe:2.3:o:freebsd:freebsd:12.0:p1:*:*:*:*:*:						
cpe:2.3:o:freebsd:freebsd:12.0:p2:*:*:*:*:*:						
cpe:2.3:o:freebsd:freebsd:12.0:p3:*:*:*:*:*:						
cpe:2.3:o:freebsd:freebsd:12.0:p4:*:*:*:*:*:						
cpe:2.3:o:freebsd:freebsd:12.0:p5:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

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](#)