

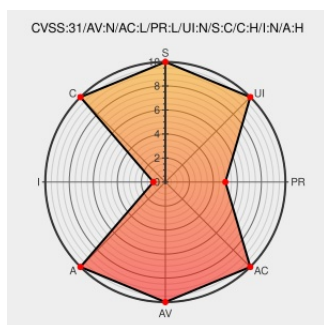


CVE-2019-5604

Published on: 07/25/2019 12:00:00 AM UTC

Last Modified on: 03/01/2023 04:20:00 PM UTC

CVE-2019-5604

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

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

In FreeBSD 12.0-STABLE before r350246, 12.0-RELEASE before 12.0-RELEASE-p8, 11.3-STABLE before r350247, 11.3-RELEASE before 11.3-RELEASE-p1, and 11.2-RELEASE before 11.2-RELEASE-p12, the emulated XHCI device included with the bhyve hypervisor did not properly validate data provided by the guest, allowing an out-of-

bounds read. This provides a malicious guest the possibility to crash the system or access system memory.

CVE-2019-5604 has been assigned by secteam@freebsd.org to track the vulnerability - currently rated as **CRITICAL** severity.

Affected Vendor/Software: **FreeBSD** - **FreeBSD** version **FreeBSD before 12.0-RELEASE-p8**

Affected Vendor/Software: **FreeBSD** - **FreeBSD** version **before 11.3-RELEASE-p1**

Affected Vendor/Software: **FreeBSD** - **FreeBSD** version **and before 11.2-RELEASE-p12**

CVSS3 Score: **9.6 - CRITICAL**

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

CVSS2 Score: **8.5 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact

COMPLETE

NONE

COMPLETE

CVE References

Description	Tags	Link
August 2019 FreeBSD Vulnerabilities in NetApp Products NetApp Product Security	security.netapp.com text/html	 CONFIRM security.netapp.com/advisory/ntap-20190814-0003/
	Third Party Advisory security.FreeBSD.org text/plain	 FREEBSD FreeBSD-SA-19:16
FreeBSD Security Advisory - FreeBSD-SA-19:16.bhyve ≈ Packet Storm	Third Party Advisory VDB Entry packetstormsecurity.com text/html	 MISC packetstormsecurity.com/files/153753/FreeBSD-Security-Advisory-FreeBSD-SA-19-16.bhyve.html

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	11.0	-	All	All
Operating System	Freebsd	Freebsd	11.2	-	All	All
Operating System	Freebsd	Freebsd	11.2	p10	All	All
Operating System	Freebsd	Freebsd	11.2	p11	All	All
Operating System	Freebsd	Freebsd	11.2	p2	All	All
Operating System	Freebsd	Freebsd	11.2	p3	All	All
Operating System	Freebsd	Freebsd	11.2	p4	All	All
Operating System	Freebsd	Freebsd	11.2	p5	All	All
Operating System	Freebsd	Freebsd	11.2	p6	All	All
Operating System	Freebsd	Freebsd	11.2	p7	All	All
Operating System	Freebsd	Freebsd	11.2	p8	All	All
Operating System	Freebsd	Freebsd	11.2	p9	All	All

Operating System	Freebsd	Freebsd	11.2	rc3	All	All
Operating System	Freebsd	Freebsd	11.3	-	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
Operating System	Freebsd	Freebsd	12.0	p6	All	All
Operating System	Freebsd	Freebsd	12.0	p7	All	All
Operating System	Freebsd	Freebsd	11.0	-	All	All
Operating System	Freebsd	Freebsd	11.2	-	All	All
Operating System	Freebsd	Freebsd	11.3	-	All	All
Operating System	Freebsd	Freebsd	12.0	-	All	All
cpe:2.3:o:freebsd:freebsd:11.0:-:*:*:*:*:*:						
cpe:2.3:o:freebsd:freebsd:11.2:-:*:*:*:*:*:						
cpe:2.3:o:freebsd:freebsd:11.2:p10:*:*:*:*:*:						
cpe:2.3:o:freebsd:freebsd:11.2:p11:*:*:*:*:*:						
cpe:2.3:o:freebsd:freebsd:11.2:p2:*:*:*:*:*:						
cpe:2.3:o:freebsd:freebsd:11.2:p3:*:*:*:*:*:						
cpe:2.3:o:freebsd:freebsd:11.2:p4:*:*:*:*:*:						
cpe:2.3:o:freebsd:freebsd:11.2:p5:*:*:*:*:*:						
cpe:2.3:o:freebsd:freebsd:11.2:p6:*:*:*:*:*:						
cpe:2.3:o:freebsd:freebsd:11.2:p7:*:*:*:*:*:						
cpe:2.3:o:freebsd:freebsd:11.2:p8:*:*:*:*:*:						

```
cpe:2.3:o:freebsd:freebsd:12.0:-:*:*:*:*:*:
```

Next ID→