



CVE-2019-5606

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

Last Modified on: 02/01/2023 02:12:00 AM UTC

CVE-2019-5606

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

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

In FreeBSD 12.0-STABLE before r349805, 12.0-RELEASE before 12.0-RELEASE-p8, 11.3-STABLE before r349806, 11.3-RELEASE before 11.3-RELEASE-p1, and 11.2-RELEASE before 11.2-RELEASE-p12, code which handles close of a descriptor created by posix_openpt fails to undo a signal configuration. This causes an incorrect signal to be raised leading to a write after free of kernel memory allowing a malicious user to gain root privileges or escape a jail.

CVE-2019-5606 has been assigned by secteam@freebsd.org to track the vulnerability - currently rated as **HIGH** 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: **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

CVE References

Description	Tags	Link
FreeBSD Security Advisory - FreeBSD-SA-19:13.pts ≈ Packet Storm	Third Party Advisory VDB Entry packetstormsecurity.com text/html	 MISC packetstormsecurity.com/files/153748/FreeBSD-Security-Advisory-FreeBSD-SA-19-13.pts.html
August 2019 FreeBSD Vulnerabilities in NetApp Products NetApp Product Security	security.netapp.com text/html	 CONFIRM security.netapp.com/advisory/ntap-20190814-0003/
	Vendor Advisory security.FreeBSD.org text/plain	 FREEBSD FreeBSD-SA-19:13

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	11.3	-	All	All
Operating System	Freebsd	Freebsd	12.0	-	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:11.3:-:*:*:*:*:*:
```

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

```
one:2.3.0:freeshd:freeshd:11 0-*.***.***.
```

cpe:2.3:o:freebsd:freebsd:11.0:-:*:*:*:*:*:
cpe:2.3:o:freebsd:freebsd:11.2:-:*:*:*:*:*:
cpe:2.3:o:freebsd:freebsd:11.3:-:*:*:*:*:*:
cpe:2.3:o:freebsd:freebsd:12.0:-:*:*:*:*:*:

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](#)