



CVE-2020-7457

Published on: 07/09/2020 12:00:00 AM UTC

Last Modified on: 01/04/2022 04:37:00 PM UTC

CVE-2020-7457

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

CVSS:31/AV:N/AC:H/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 r359565, 12.1-RELEASE before p7, 11.4-STABLE before r362975, 11.4-RELEASE before p1, and 11.3-RELEASE before p11, missing synchronization in the IPV6_2292PKTOPTIONS socket option set handler contained a race condition allowing a malicious application to modify memory after being freed, possibly resulting in code execution.

CVE-2020-7457 has been assigned by secteam@freebsd.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **8.1 - HIGH**

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

CVSS2 Score: **6.8 - MEDIUM**

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

CVE References

Description	Tags	Link
July 2020 FreeBSD Vulnerabilities in NetApp Products NetApp Product Security	security.netapp.com text/html	CONFIRM security.netapp.com/advisory/ntap-20200724-0002/

[Patch](#)
[Vendor Advisory](#)
[security.FreeBSD.org](#)
[text/plain](#)

 [MISC security.FreeBSD.org/advisories/FreeBSD-SA-20:20.ipv6.asc](https://security.FreeBSD.org/advisories/FreeBSD-SA-20:20.ipv6.asc)

FreeBSD ip6_setpktopt Use-After-Free Privilege Escalation ≈ Packet Storm

[packetstormsecurity.com](#)
[text/html](#)

 [MISC packetstormsecurity.com/files/158695/FreeBSD-ip6_setpktopt-Use-After-Free-Privilege-Escalation.html](https://packetstormsecurity.com/files/158695/FreeBSD-ip6_setpktopt-Use-After-Free-Privilege-Escalation.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	11.3	-	All	All
Operating System	Freebsd	Freebsd	11.3	p1	All	All
Operating System	Freebsd	Freebsd	11.3	p10	All	All
Operating System	Freebsd	Freebsd	11.3	p2	All	All
Operating System	Freebsd	Freebsd	11.3	p3	All	All
Operating System	Freebsd	Freebsd	11.3	p4	All	All
Operating System	Freebsd	Freebsd	11.3	p5	All	All
Operating System	Freebsd	Freebsd	11.3	p6	All	All
Operating System	Freebsd	Freebsd	11.3	p7	All	All
Operating System	Freebsd	Freebsd	11.3	p8	All	All
Operating System	Freebsd	Freebsd	11.3	p9	All	All
Operating System	Freebsd	Freebsd	11.4	-	All	All
Operating System	Freebsd	Freebsd	11.4	beta1	All	All
Operating System	Freebsd	Freebsd	11.4	rc2	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
Operating System	Freebsd	Freebsd	12.1	p5	All	All
Operating System	Freebsd	Freebsd	12.1	p6	All	All
Operating System	Freebsd	Freebsd	11.3	-	All	All
Operating System	Freebsd	Freebsd	11.3	p1	All	All
Operating System	Freebsd	Freebsd	11.3	p10	All	All
Operating System	Freebsd	Freebsd	11.3	p2	All	All
Operating System	Freebsd	Freebsd	11.3	p3	All	All
Operating System	Freebsd	Freebsd	11.3	p4	All	All
Operating System	Freebsd	Freebsd	11.3	p5	All	All
Operating System	Freebsd	Freebsd	11.3	p6	All	All
Operating System	Freebsd	Freebsd	11.3	p7	All	All
Operating System	Freebsd	Freebsd	11.3	p8	All	All
Operating System	Freebsd	Freebsd	11.3	p9	All	All
Operating System	Freebsd	Freebsd	11.4	-	All	All
Operating System	Freebsd	Freebsd	11.4	beta1	All	All
Operating System	Freebsd	Freebsd	11.4	rc2	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
Operating System	Freebsd	Freebsd	12.1	p5	All	All
Operating System	Freebsd	Freebsd	12.1	p6	All	All
cpe:2.3:o:freebsd:freebsd:11.3:-:*:*:*:*:*:						
cpe:2.3:o:freebsd:freebsd:11.3:p1:*:*:*:*:*:						
cpe:2.3:o:freebsd:freebsd:11.3:p10:*:*:*:*:*:						
cpe:2.3:o:freebsd:freebsd:11.3:p2:*:*:*:*:*:						
cpe:2.3:o:freebsd:freebsd:11.3:p3:*:*:*:*:*:						
cpe:2.3:o:freebsd:freebsd:11.3:p4:*:*:*:*:*:						
cpe:2.3:o:freebsd:freebsd:11.3:p5:*:*:*:*:*:						
cpe:2.3:o:freebsd:freebsd:11.3:p6:*:*:*:*:*:						
cpe:2.3:o:freebsd:freebsd:11.3:p7:*:*:*:*:*:						
cpe:2.3:o:freebsd:freebsd:11.3:p8:*:*:*:*:*:						
cpe:2.3:o:freebsd:freebsd:11.3:p9:*:*:*:*:*:						
cpe:2.3:o:freebsd:freebsd:11.4:-:*:*:*:*:*:						
cpe:2.3:o:freebsd:freebsd:11.4:beta1:*:*:*:*:*:						
cpe:2.3:o:freebsd:freebsd:11.4:rc2:*:*:*:*:*:						
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:p5:*:*:*:*:*:						
cpe:2.3:o:freebsd:freebsd:12.1:p6:*:*:*:*:*:						
cpe:2.3:o:freebsd:freebsd:11.3:-:*:*:*:*:*:						
cpe:2.3:o:freebsd:freebsd:11.3:p1:*:*:*:*:*:						

cpe:2.3:o:freebsd:freebsd:11.3:p10:~::~~::~~::~~::~~::~~::
cpe:2.3:o:freebsd:freebsd:11.3:p2:~::~~::~~::~~::~~::~~::
cpe:2.3:o:freebsd:freebsd:11.3:p3:~::~~::~~::~~::~~::~~::
cpe:2.3:o:freebsd:freebsd:11.3:p4:~::~~::~~::~~::~~::~~::
cpe:2.3:o:freebsd:freebsd:11.3:p5:~::~~::~~::~~::~~::~~::
cpe:2.3:o:freebsd:freebsd:11.3:p6:~::~~::~~::~~::~~::~~::
cpe:2.3:o:freebsd:freebsd:11.3:p7:~::~~::~~::~~::~~::~~::
cpe:2.3:o:freebsd:freebsd:11.3:p8:~::~~::~~::~~::~~::~~::
cpe:2.3:o:freebsd:freebsd:11.3:p9:~::~~::~~::~~::~~::~~::
cpe:2.3:o:freebsd:freebsd:11.4:-:~::~~::~~::~~::~~::~~::
cpe:2.3:o:freebsd:freebsd:11.4:beta1:~::~~::~~::~~::~~::~~::
cpe:2.3:o:freebsd:freebsd:11.4:rc2:~::~~::~~::~~::~~::~~::
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:p5:~::~~::~~::~~::~~::~~::
cpe:2.3:o:freebsd:freebsd:12.1:p6:~::~~::~~::~~::~~::~~::

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)