



CVE-2020-7469

Published on: 06/04/2021 12:00:00 AM UTC

Last Modified on: 05/31/2022 03:54:00 PM UTC

CVE-2020-7469

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

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



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

In FreeBSD 12.2-STABLE before r367402, 11.4-STABLE before r368202, 12.2-RELEASE before p1, 12.1-RELEASE before p11 and 11.4-RELEASE before p5 the handler for a routing option caches a pointer into the packet buffer holding the ICMPv6 message. However, when processing subsequent options the packet buffer may be freed, rendering the cached pointer invalid. The network stack may later dereference the pointer, potentially triggering a use-after-free.

CVE-2020-7469 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: **5 - MEDIUM**

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

CVE References

Description	Tags	Link
-------------	------	------

CVE-2020-7469 FreeBSD Vulnerability in NetApp Products

[CVE-2020-7469](#)

[CONFIRM security-notepad.com/advisory/2021-06-04-cve-2020-7469-freebsd-vulnerability-in-netapp-products](#)

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.

Related QID Numbers

[690389](#) Free Berkeley Software Distribution (FreeBSD) Security Update for (8eed0c5c-3482-11eb-b87a-901b0ef719ab)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Freebsd	Freebsd	11.4	-	All	All
Operating System	Freebsd	Freebsd	11.4	beta1	All	All
Operating System	Freebsd	Freebsd	11.4	p1	All	All
Operating System	Freebsd	Freebsd	11.4	p2	All	All
Operating System	Freebsd	Freebsd	11.4	p3	All	All
Operating System	Freebsd	Freebsd	11.4	p4	All	All
Operating System	Freebsd	Freebsd	11.4	rc1	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	p10	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	12.1	p/	All	All
Operating System	Freebsd	Freebsd	12.1	p8	All	All
Operating System	Freebsd	Freebsd	12.1	p9	All	All
Operating System	Freebsd	Freebsd	12.2	-	All	All
Application	Netapp	Clustered Data Ontap	-	All	All	All
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:p1:*:*:*:*:*:						
cpe:2.3:o:freebsd:freebsd:11.4:p2:*:*:*:*:*:						
cpe:2.3:o:freebsd:freebsd:11.4:p3:*:*:*:*:*:						
cpe:2.3:o:freebsd:freebsd:11.4:p4:*:*:*:*:*:						
cpe:2.3:o:freebsd:freebsd:11.4:rc1:*:*:*:*:*:						
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:p10:*:*:*:*:*:						
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:12.1:p7:*:*:*:*:*:						
cpe:2.3:o:freebsd:freebsd:12.1:p8:*:*:*:*:*:						
cpe:2.3:o:freebsd:freebsd:12.1:p9:*:*:*:*:*:						
cpe:2.3:o:freebsd:freebsd:12.2:-:*:*:*:*:*:						
cpe:2.3:a:netapp:clustered_data_ontap:-:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2020-7469 : In FreeBSD 12.2-STABLE before r367402, 11.4-STABLE before r368202, 12.2-RELEASE before p1, 12.1-REL... twitter.com/i/web/status/1...	2021-06-04 12:05:50
 @LinInfoSec	Freebsd - CVE-2020-7469: security.FreeBSD.org/advisories/Fre...	2021-06-04 14:32:01
 @threatmeter	CVE-2020-7469 In FreeBSD 12.2-STABLE before r367402, 11.4-STABLE before r368202, 12.2-RELEASE before p1, 12.1-RELEA... twitter.com/i/web/status/1...	2021-06-05 07:10:33
 /r/netcve	CVE-2020-7469	2021-06-04 12:41:24

[← 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](#)