



CVE-2020-7453

Published on: 04/28/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:55 PM UTC

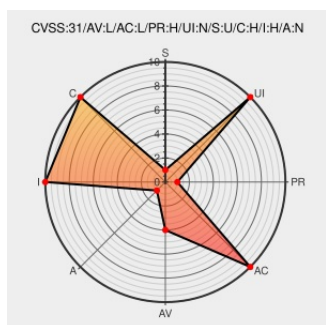
CVE-2020-7453

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



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

In FreeBSD 12.1-STABLE before r359021, 12.1-RELEASE before 12.1-RELEASE-p3, 11.3-STABLE before r359020, and 11.3-RELEASE before 11.3-RELEASE-p7, a missing null termination check in the jail_set configuration option "osrelease" may return more bytes with a subsequent jail_get system call allowing a malicious jail superuser with permission to create nested jails to read kernel memory.

CVE-2020-7453 has been assigned by secteam@freebsd.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **6 - MEDIUM**

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

CVSS2 Score: **3.3 - LOW**

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

CVE References

Description	Tags	Link
	Patch Vendor Advisory	CONFIRM security.FreeBSD.org/advisories/FreeBSD-SA-20:08.jail.asc

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	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	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	11.3	-	All	All
Operating System	Freebsd	Freebsd	11.3	p1	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	12.1	-	All	All
Operating System	Freebsd	Freebsd	12.1	p1	All	All
Operating System	Freebsd	Freebsd	12.1	p2	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: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: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:11.3:-:*:*:*:*:*:						
cpe:2.3:o:freebsd:freebsd:11.3:p1:*:*:*:*:*:						
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:12.1:-:*:*:*:*:*:						
cpe:2.3:o:freebsd:freebsd:12.1:p1:*:*:*:*:*:						
cpe:2.3:o:freebsd:freebsd:12.1:p2:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

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](#)