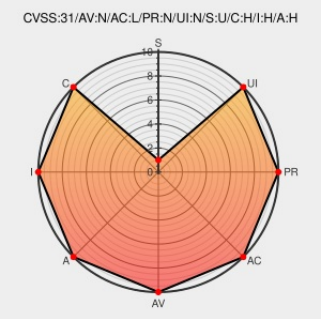
CVE-2020-7458

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

Last Modified on: 01/04/2022 04:39:00 PM UTC

CVE-2020-7458

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Freebsd from Freebsd contain the following vulnerability:

In FreeBSD 12.1-STABLE before r362281, 11.4-STABLE before r362281, and 11.4-RELEASE before p1, long values in the user-controlled PATH environment variable cause posix_spawnp to write beyond the end of the heap allocated stack possibly leading to arbitrary code execution.

CVE-2020-7458 has been assigned by secteam@freebsd.org to track the vulnerability - currently rated as CRITICAL severity.

CVSS3 Score: 9.8 - CRITICAL

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

CVSS2 Score: 7.5 - HIGH

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

CVE References

Description	Tags	Link
	Patch Vendor Advisory security.FreeBSD.org	MISC security.FreeBSD.org/advisories/FreeBSD-SA-20:18.posix_spawnp.asc

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

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	11.4	-	All	All
Operating System	Freebsd	Freebsd	11.4	beta1	All	All
Operating System	Freebsd	Freebsd	12.1	-	All	All
Operating System	Freebsd	Freebsd	11.4	-	All	All
Operating System	Freebsd	Freebsd	11.4	beta1	All	All
Operating System	Freebsd	Freebsd	12.1	-	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:12.1:-:*:*:*:*:*:*:

cpe:2.3:o:freebsd:freebsd:11.4:-:*:*:*:*:*:*:

cpe:2.3:o:freebsd:freebsd:11.4:beta1:*:*:*:*:*:*:

cpe:2.3:o:freebsd:freebsd:12.1:-:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report