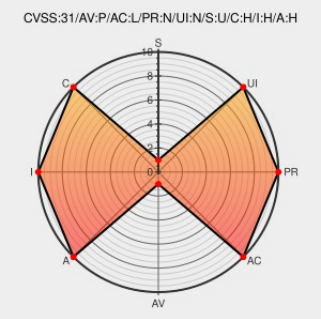
CVE-2020-7456

Published on: 06/09/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:54 PM UTC

CVE-2020-7456

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



Certain versions of Freebsd from Freebsd contain the following vulnerability:

In FreeBSD 12.1-STABLE before r361918, 12.1-RELEASE before p6, 11.4-STABLE before r361919, 11.3-RELEASE before p10, and 11.4-RC2 before p1, an invalid memory location may be used for HID items if the push/pop level is not restored within the processing of that HID item allowing an attacker with physical access to a USB port to be able to use a specially crafted USB device to gain kernel or user-space code execution.

CVE-2020-7456 has been assigned by secteam@freebsd.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 6.8 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
PHYSICAL	LOW	NONE	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**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
CVE-2020-7456 FreeBSD Vulnerability in NetApp Products | NetApp Product Security	Third Party Advisory security.netapp.com	CONFIRM security.netapp.com/advisory/ntap-20200625-

	text/html	0005/
	Patch Vendor Advisory security.FreeBSD.org text/plain	MISC security.FreeBSD.org/advisories/FreeBSD-SA-20:17.usb.asc

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	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	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	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	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	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	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	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
Application	Netapp	Clustered Data Ontap	-	All	All	All
Application	Netapp	Clustered Data Ontap	-	All	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: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: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: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: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: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: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: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:a:netapp:clustered_data_ontap:-:*:*:*:*:*:*:*:

cpe:2.3:a:netapp:clustered_data_ontap:-:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→