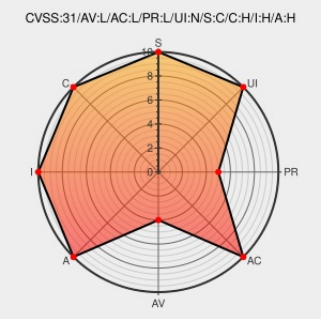
CVE-2017-5123

Published on: 11/02/2021 12:00:00 AM UTC

Last Modified on: 04/18/2022 06:03:00 PM UTC

CVE-2017-5123

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



Certain versions of Linux Kernel from Linux contain the following vulnerability:

Insufficient data validation in waitid allowed an user to escape sandboxes on Linux.

CVE-2017-5123 has been assigned by chrome-cve-admin@google.com to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.8 - HIGH

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

CVSS2 Score: 4.6 - MEDIUM

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

CVE References

Description	Tags	Link
772848 - chromium - An open-source project to help move the web forward. - Monorail	crbug.com text/html	MISC crbug.com/772848
CVE-2017-5123 Linux Kernel Vulnerability in NetApp Products | NetApp Product Security	security.netapp.com text/html	CONFIRM security.netapp.com/advisory/ntap-20211223-0003/

kernel/git/torvalds/linux.git - Linux kernel source tree	git.kernel.org text/html	MISC git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=96ca579a1ecc943b75beba58bebb0356f6cc4b51

There are currently no QIDs associated with this CVE

Exploit/POC from Github

Exploit for the linux kernel vulnerability CVE-2017-5123

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	All	All	All	All
Application	Netapp	Cloud Backup	-	All	All	All
Hardware	Netapp	H300e	-	All	All	All
Operating System	Netapp	H300e Firmware	-	All	All	All
Hardware	Netapp	H300s	-	All	All	All
Operating System	Netapp	H300s Firmware	-	All	All	All
Hardware	Netapp	H410s	-	All	All	All
Operating System	Netapp	H410s Firmware	-	All	All	All
Hardware	Netapp	H500e	-	All	All	All
Operating System	Netapp	H500e Firmware	-	All	All	All
Hardware	Netapp	H500s	-	All	All	All
Operating System	Netapp	H500s Firmware	-	All	All	All
Hardware	Netapp	H700e	-	All	All	All
Operating System	Netapp	H700e Firmware	-	All	All	All
Hardware	Netapp	H700s	-	All	All	All
Operating System	Netapp	H700s Firmware	-	All	All	All

cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*:*:

cpe:2.3:a:netapp:cloud_backup:-:*:*:*:*:*:*:*:

cpe:2.3:h:netapp:h300e:-:*:*:*:*:*:*:*:

cpe:2.3:o:netapp:h300e_firmware:-:*:*:*:*:*:*:*:

cpe:2.3:h:netapp:h300s:-:*:*:*:*:*:*:*:

cpe:2.3:o:netapp:h300s_firmware:-:*:*:*:*:*:*:*:

cpe:2.3:h:netapp:h410s:-:*:*:*:*:*:*:*:

cpe:2.3:o:netapp:h410s_firmware:-:*:*:*:*:*:*:*:

cpe:2.3:h:netapp:h500e:-:*:*:*:*:*:*:*:

cpe:2.3:o:netapp:h500e_firmware:-:*:*:*:*:*:*:*:

cpe:2.3:h:netapp:h500s:-:*:*:*:*:*:*:*:

cpe:2.3:o:netapp:h500s_firmware:-:*:*:*:*:*:*:*:

cpe:2.3:h:netapp:h700e:-:*:*:*:*:*:*:*:

cpe:2.3:o:netapp:h700e_firmware:-:*:*:*:*:*:*:*:

cpe:2.3:h:netapp:h700s:-:*:*:*:*:*:*:*:

cpe:2.3:o:netapp:h700s_firmware:-:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@GrupoICA_Ciber	?LINUX? Múltiples vulnerabilidades de severidad alta en productos LINUX: CVE-2017-5123,CVE-2021-43267,CVE-2021-42… twitter.com/i/web/status/1…	2021-11-05 09:16:11

← Previous ID

Next ID→