

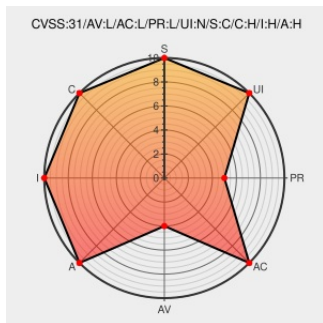


CVE-2017-5123

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	cbug.com text/html	MISC cbug.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](#)



git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit?id=96ca579a1ecc943b75beba58bebb0356f6cc4b51

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

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)
 @GrupolCA_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→

© 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