



CVE-2017-11472

Published on: 07/20/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:24 PM UTC

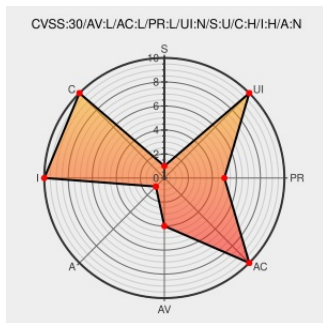
CVE-2017-11472

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



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

The `acpi_ns_terminate()` function in `drivers/acpi/acpica/nsutils.c` in the Linux kernel before 4.12 does not flush the operand cache and causes a kernel stack dump, which allows local users to obtain sensitive information from kernel memory and bypass the KASLR protection mechanism (in the kernel through 4.9) via a crafted ACPI table.

CVE-2017-11472 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.1 - HIGH**

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

CVSS2 Score: **3.6 - LOW**

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

CVE References

Description	Tags	Link
kernel/git/torvalds/linux.git - Linux kernel source tree	Issue Tracking Patch Third Party Advisory	CONFIRM git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=3b2d69114fefa474fca542e51119036dceb4aa6f

	git.kernel.org text/html	
Namespace: fix operand cache leak · acpica/acpica@a23325b · GitHub	Issue Tracking Patch Third Party Advisory github.com text/html	 CONFIRM github.com/acpica/acpica/commit/a23325b2e583556eae88ed3f764e457786bf4df6
USN-3619-1: Linux kernel vulnerabilities Ubuntu security notices	usn.ubuntu.com text/html	 UBUNTU USN-3619-1
USN-3619-2: Linux kernel (Xenial HWE) vulnerabilities Ubuntu security notices	usn.ubuntu.com text/html	 UBUNTU USN-3619-2
USN-3754-1: Linux kernel vulnerabilities Ubuntu security notices Ubuntu	usn.ubuntu.com text/html	 UBUNTU USN-3754-1
ACPICA: Namespace: fix operand cache leak · torvalds/linux@3b2d691 · GitHub	Issue Tracking Patch Third Party Advisory github.com text/html	 CONFIRM github.com/torvalds/linux/commit/3b2d69114fefa474fca542e51119036dceb4aa6f

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	Linux	Linux Kernel	All	All	All	All
cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)