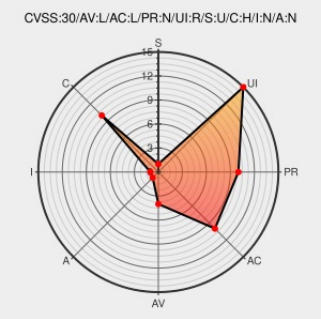
CVE-2016-7914

Published on: 11/15/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:06 PM UTC

CVE-2016-7914

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



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

The assoc_array_insert_into_terminal_node function in lib/assoc_array.c in the Linux kernel before 4.5.3 does not check whether a slot is a leaf, which allows local users to obtain sensitive information from kernel memory or cause a denial of service (invalid pointer dereference and out-of-bounds read) via an application that uses associative-array data structures, as demonstrated by the keyutils test suite.

CVE-2016-7914 has been assigned by security@android.com to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 5.5 - MEDIUM

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

CVSS2 Score: 7.1 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	NONE	NONE

CVE References

Description	Tags	Link
assoc_array: don't call compare_object() on a	Issue Tracking Patch	CONFIRM github.com/torvalds/linux/commit/8d4a2ec1e0b41b0cf9a0c5cd4511da7f8e4f3de2

node · torvalds/linux@8d4a2ec · GitHub	Third Party Advisory github.com text/html	
Android Security Bulletin—November 2016 | Android Open Source Project	Third Party Advisory source.android.com text/html	CONFIRM source.android.com/security/bulletin/2016-11-01.html
kernel/git/torvalds/linux.git - Linux kernel source tree	Issue Tracking Patch Third Party Advisory git.kernel.org text/html	CONFIRM git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=8d4a2ec1e0b41b0cf9a0c5cd4511da7f8e4f3de2
	Release Notes www.kernel.org text/plain	CONFIRM www.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.5.3
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2016:2574
Linux Kernel Multiple Information Disclosure Vulnerabilities	Third Party Advisory VDB Entry cve.report (archive) text/html	BID 94138

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→