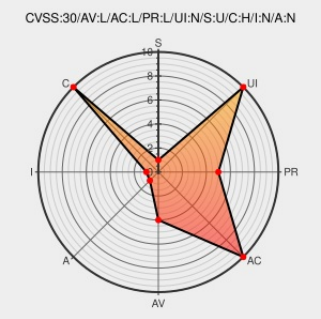
CVE-2016-9178

Published on: 11/27/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:17 PM UTC

CVE-2016-9178

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



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

The __get_user_asm_ex macro in arch/x86/include/asm/uaccess.h in the Linux kernel before 4.7.5 does not initialize a certain integer variable, which allows local users to obtain sensitive information from kernel stack memory by triggering failure of a get_user_ex call.

CVE-2016-9178 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 5.5 - MEDIUM

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

CVSS2 Score: 2.1 - LOW

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

CVE References

Description	Tags	Link
fix minor infoleak in get_user_ex() · torvalds/linux@1c109fa · GitHub	Issue Tracking, Patch, Third Party Advisory, github.com, text/html	CONFIRM github.com/torvalds/linux/commit/1c109fabbd51863475cd12ac206bdd249aee35af

	Release Notes www.kernel.org text/plain	CONFIRM www.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.7.5
Linux Kernel CVE-2016-9178 Local Information Disclosure Vulnerability	cve.report (archive) text/html	BID 94144
oss-security - Re: kernel: fix minor infoleak in get_user_ex()	Mailing List Third Party Advisory www.openwall.com text/html	MLIST [oss-security] 20161104 Re: kernel: fix minor infoleak in get_user_ex()
Bug 1391908 – CVE-2016-9178 kernel: Information leak in get_user_ex function	Issue Tracking bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=1391908
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=1c109fabbd51863475cd12ac206bdd249aee35af

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→