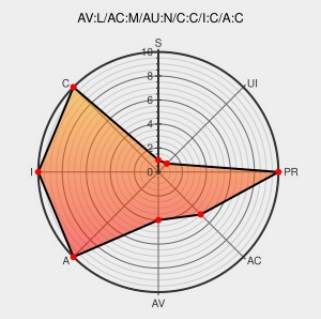
CVE-2015-2666

Published on: 05/27/2015 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:20 PM UTC

CVE-2015-2666

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



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

Stack-based buffer overflow in the get_matching_model_microcode function in arch/x86/kernel/cpu/microcode/intel_early.c in the Linux kernel before 4.0 allows context-dependent attackers to gain privileges by constructing a crafted microcode header and leveraging root privileges for write access to the initrd.

CVE-2015-2666 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 6.9 - MEDIUM

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

CVE References

Description	Tags	Link
x86/microcode/intel: Guard against stack overflow in the loader · torvalds/linux@f84598b · GitHub	github.com text/html	CONFIRM github.com/torvalds/linux/commit/f84598bd7c851f8b0bf8cd0d7c3be0d73c43
Linux Kernel Buffer Overflow in get_matching_model_microcode() Lets Local Users Gain Elevated Privileges - SecurityTracker	www.securitytracker.com text/html	SECTRACK 1032414
kernel/git/torvalds/linux.git - Linux kernel source tree	git.kernel.org text/html	CONFIRM git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=f84598bd7c851f8b0bf8cd0d7c3be0d73c432ff4
Bug 1204722 – CVE-2015-2666 kernel: execution in the early	bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=1204722

microcode loader		
oss-security - Re: CVE Request: Linux kernel execution in the early microcode loader.	www.openwall.com text/html	MLIST [oss-security] 20150320 Re: CVE Request: Linux kernel execution the early microcode loader.
[SECURITY] Fedora 21 Update: kernel-3.19.2-201.fc21	lists.fedoraproject.org text/html	FEDORA FEDORA-2015-4457
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2015:1534

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→