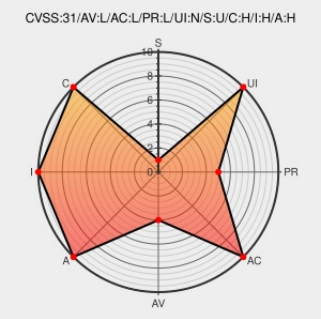
CVE-2015-3288

Published on: 10/16/2016 12:00:00 AM UTC

Last Modified on: 02/12/2023 11:15:00 PM UTC

CVE-2015-3288

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



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

mm/memory.c in the Linux kernel before 4.1.4 mishandles anonymous pages, which allows local users to gain privileges or cause a denial of service (page tainting) via a crafted application that triggers writing to page zero.

CVE-2015-3288 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.8 - HIGH

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

CVSS2 Score: 7.2 - HIGH

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

CVE References

Description	Tags	Link
CVE-2015-3288 - Red Hat Customer Portal	access.redhat.com text/html	MISC access.redhat.com/security/cve/CVE-2015-3288
Android Security Bulletin—January 2017 | Android	source.android.com text/html	CONFIRM source.android.com/security/bulletin/2017-01-01.html

Open Source Project		
Linux Kernel 'mm/memory.c' Local Code Execution Vulnerability	cve.report (archive) text/html	BID 93591
	Release Notes Vendor Advisory www.kernel.org text/plain	CONFIRM www.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.1.4
CVE-2015-3288	Third Party Advisory security-tracker.debian.org text/html	CONFIRM security-tracker.debian.org/tracker/CVE-2015-3288
Red Hat Customer Portal	access.redhat.com text/html	MISC access.redhat.com/errata/RHSA-2015:2152
kernel/git/torvalds/linux.git - Linux kernel source tree	Patch Vendor Advisory git.kernel.org text/html	CONFIRM git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=6b7339f4c31ad69c8e9c0b2859276e22cf72176d
Bug 1333830 – CVE-2015-3288 kernel: zero page memory arbitrary modification	Issue Tracking Patch Third Party Advisory VDB Entry bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=1333830
mm: avoid setting up anonymous pages into file mapping · torvalds/linux@6b7339f · GitHub	Vendor Advisory github.com text/html	CONFIRM github.com/torvalds/linux/commit/6b7339f4c31ad69c8e9c0b2859276e22cf72176d

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
Operating System	Linux	Linux Kernel	All	All	All	All

cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report