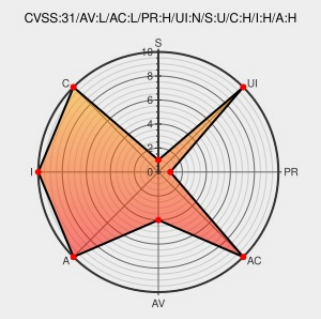
CVE-2015-8660

Published on: 12/28/2015 12:00:00 AM UTC

Last Modified on: 06/07/2023 12:44:00 PM UTC

CVE-2015-8660

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



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

The ovl_setattr function in fs/overlayfs/inode.c in the Linux kernel through 4.3.3 attempts to merge distinct setattr operations, which allows local users to bypass intended access restrictions and modify the attributes of arbitrary overlay files via a crafted application.

CVE-2015-8660 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 6.7 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	HIGH	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
oss-security - CVE request -- linux kernel: overlay: fix permission checking for setattr	www.openwall.com text/html	MLIST [oss-security] 20151223 CVE request -- linux kernel: overlay: fix permission checking for setattr

Linux Kernel 4.3.3 - 'overlayfs' Privilege Escalation (2)	www.exploit-db.com Proof of Concept text/html	EXPLOIT-DB 39230
USN-2858-3: Linux kernel (Raspberry Pi 2) vulnerability | Ubuntu	www.ubuntu.com text/html	UBUNTU USN-2858-3
USN-2858-1: Linux kernel vulnerability | Ubuntu	www.ubuntu.com text/html	UBUNTU USN-2858-1
Red Hat Customer Portal	access.redhat.com text/html	MISC access.redhat.com/errata/RHSA-2016:1532
Oracle Linux Bulletin - July 2016	web.archive.org text/html Inactive Link Not Archived	CONFIRM www.oracle.com/technetwork/topics/security/linuxbulletinjul2016-3090544.html
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2016:1539
USN-2857-2: Linux kernel (Vivid HWE) vulnerability | Ubuntu	www.ubuntu.com text/html	UBUNTU USN-2857-2
[security-announce] SUSE-SU-2016:0752-1: important: Security update for	lists.opensuse.org text/html	SUSE SUSE-SU-2016:0752
CVE-2015-8660 - Red Hat Customer Portal	access.redhat.com text/html	MISC access.redhat.com/security/cve/CVE-2015-8660
ovl: fix permission checking for setattr · torvalds/linux@acff81e · GitHub	github.com text/html	CONFIRM github.com/torvalds/linux/commit/acff81ec2c79492b180fade3c2894425cd35a545
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2016:1541
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2016:1532
Bug 1291329 – CVE-2015-8660 kernel: Permission bypass on overlayfs during copy_up	bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=1291329
Oracle VM Server for x86 Bulletin - July 2016	web.archive.org text/html Inactive Link Not Archived	CONFIRM www.oracle.com/technetwork/topics/security/ovmbulletinjul2016-3090546.html
[security-announce] SUSE-SU-2016:0755-1: important: Security update for	lists.opensuse.org text/html	SUSE SUSE-SU-2016:0755
[security-announce] SUSE-SU-2016:0751-1: important: Security update for	lists.opensuse.org text/html	SUSE SUSE-SU-2016:0751
USN-2857-1: Linux kernel vulnerability | Ubuntu	www.ubuntu.com text/html	UBUNTU USN-2857-1
Linux Kernel Overlayfs Security Permissions Flaw	www.securitytracker.com text/html	SECTRACK 1034548

Lets Local Users Bypass Security Restrictions - SecurityTracker		
Linux Kernel (Ubuntu / Fedora / RedHat) - 'Overlayfs' Privilege Escalation (Metasploit)	www.exploit-db.com Proof of Concept text/html	EXPLOIT-DB 40688
Linux Kernel 'fs/overlayfs/inode.c' Local Privilege Escalation Vulnerability	cve.report (archive) text/html	BID 79671
kernel/git/torvalds/linux.git - Linux kernel source tree	git.kernel.org text/html	CONFIRM git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=acff81ec2c79492b180fade3c2894425cd35a545
Red Hat Customer Portal	access.redhat.com text/html	MISC access.redhat.com/errata/RHSA-2016:1541
USN-2858-2: Linux kernel (Wily HWE) vulnerability | Ubuntu	www.ubuntu.com text/html	UBUNTU USN-2858-2
Ubuntu 14.04 LTS / 15.10 overlayfs Local Root ≈ Packet Storm	packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/135151/Ubuntu-14.04-LTS-15.10-overlayfs-Local-Root.html
Ubuntu 14.04 LTS, 15.10 overlayfs - Local Root Exploit	www.exploit-db.com Proof of Concept text/html	EXPLOIT-DB 39166
Red Hat Customer Portal	access.redhat.com text/html	MISC access.redhat.com/errata/RHSA-2016:1539

There are currently no QIDs associated with this CVE

Exploit/POC from Github

这个代码包含了CVE-2015-8660漏洞的利用代码，还有注释，出现问题的源代码，打了补丁后的代码

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→