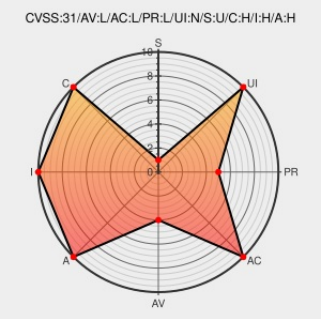
CVE-2016-0758

Published on: 06/27/2016 12:00:00 AM UTC

Last Modified on: 02/12/2023 11:16:00 PM UTC

CVE-2016-0758

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



Certain versions of Ubuntu Linux from Canonical contain the following vulnerability:

Integer overflow in lib/asn1_decoder.c in the Linux kernel before 4.6 allows local users to gain privileges via crafted ASN.1 data.

CVE-2016-0758 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
[security-announce] SUSE-SU-2016:2001-1: important: Security update for	lists.opensuse.org text/html	SUSE SUSE-SU-2016:2001
[security-announce] SUSE-	lists.opensuse.org	SUSE SUSE-SU-2016:2009

SU-2016:2009-1: important: Security update for	text/html	
Red Hat Customer Portal	access.redhat.com text/html	MISC access.redhat.com/errata/RHSA-2016:1055
[security-announce] SUSE-SU-2016:1961-1: important: Security update for	lists.opensuse.org text/html	SUSE SUSE-SU-2016:1961
CVE-2016-0758 - Red Hat Customer Portal	access.redhat.com text/html	MISC access.redhat.com/security/cve/CVE-2016-0758
Red Hat Customer Portal	access.redhat.com text/html	MISC access.redhat.com/errata/RHSA-2016:1051
[security-announce] SUSE-SU-2016:1937-1: important: Security update for	lists.opensuse.org text/html	SUSE SUSE-SU-2016:1937
[security-announce] SUSE-SU-2016:2010-1: important: Security update for	lists.opensuse.org text/html	SUSE SUSE-SU-2016:2010
[security-announce] SUSE-SU-2016:2005-1: important: Security update for	lists.opensuse.org text/html	SUSE SUSE-SU-2016:2005
[security-announce] SUSE-SU-2016:2002-1: important: Security update for	lists.opensuse.org text/html	SUSE SUSE-SU-2016:2002
[security-announce] openSUSE-SU-2016:1641-1: important: Security update	lists.opensuse.org text/html	SUSE openSUSE-SU-2016:1641
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2016:1055
USN-2979-4: Linux kernel (Qualcomm Snapdragon) vulnerability | Ubuntu	www.ubuntu.com text/html	UBUNTU USN-2979-4
Red Hat Customer Portal	access.redhat.com text/html	MISC access.redhat.com/errata/RHSA-2016:1033
[security-announce] SUSE-SU-2016:2007-1: important: Security update for	lists.opensuse.org text/html	SUSE SUSE-SU-2016:2007
[security-announce] SUSE-SU-2016:1985-1: important: Security update for	lists.opensuse.org text/html	SUSE SUSE-SU-2016:1985
kernel/git/torvalds/linux.git - Linux kernel source tree	Vendor Advisory git.kernel.org text/html	CONFIRM git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=23c8a812dc3c621009e4f0e5342aa4e2ede1ceaa
[security-announce] SUSE-SU-2016:1994-1: important: Security update for	lists.opensuse.org text/html	SUSE SUSE-SU-2016:1994
1300257 – (CVE-2016-0758) CVE-2016-0758 kernel: tags with indefinite length can corrupt pointers in asn1_find_indefinite_length()	bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=1300257

[security-announce] SUSE-SU-2016:1995-1: important: Security update for	lists.opensuse.org text/html	SUSE SUSE-SU-2016:1995
Oracle Linux Bulletin - April 2016	www.oracle.com text/html	CONFIRM www.oracle.com/technetwork/topics/security/linuxbulletinapr2016-2952096.html
[security-announce] SUSE-SU-2016:2014-1: important: Security update for	lists.opensuse.org text/html	SUSE SUSE-SU-2016:2014
Android Security Bulletin—October 2016 | Android Open Source Project	source.android.com text/html	CONFIRM source.android.com/security/bulletin/2016-10-01.html
Linux Kernel 'lib/asn1_decoder.c' Local Memory Corruption Vulnerability	cve.report (archive) text/html	BID 90626
[security-announce] SUSE-SU-2016:1672-1: important: Security update for	lists.opensuse.org text/html	SUSE SUSE-SU-2016:1672
KEYS: Fix ASN.1 indefinite length object parsing · torvalds/linux@23c8a81 · GitHub	Vendor Advisory github.com text/html	CONFIRM github.com/torvalds/linux/commit/23c8a812dc3c621009e4f0e5342aa4e2ede1cea
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2016:1051
[security-announce] SUSE-SU-2016:2006-1: important: Security update for	lists.opensuse.org text/html	SUSE SUSE-SU-2016:2006
oss-security - CVE-2016-0758 - Linux kernel - Flaw in ASN.1 DER decoder for x509 certificate DER files.	www.openwall.com text/html	MLIST [oss-security] 20160513 CVE-2016-0758 - Linux kernel - Flaw in ASN.1 DER decoder for x509 certificate DER files.
No Description Provided	h20565.www2.hp.com text/html	HP HPSBHF3548
[security-announce] SUSE-SU-2016:2003-1: important: Security update for	lists.opensuse.org text/html	SUSE SUSE-SU-2016:2003
[security-announce] SUSE-SU-2016:1690-1: important: Security update for	lists.opensuse.org text/html	SUSE SUSE-SU-2016:1690
[security-announce] SUSE-SU-2016:2105-1: important: Security update for	lists.opensuse.org text/html	SUSE SUSE-SU-2016:2105
[security-announce] SUSE-SU-2016:2011-1: important: Security update for	lists.opensuse.org text/html	SUSE SUSE-SU-2016:2011
[security-announce] openSUSE-SU-2016:2184-1: important: Security update	lists.opensuse.org text/html	SUSE openSUSE-SU-2016:2184
[security-announce] SUSE-SU-2016:2000-1: important:	lists.opensuse.org text/html	SUSE SUSE-SU-2016:2000

Security update for		
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2016:1033

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	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Hpc Node	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Hpc Node	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Hpc Node Eus	7.2	All	All	All
Operating System	Redhat	Enterprise Linux Hpc Node Eus	7.2	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.2	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.2	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.2	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.2	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All

Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All

cpe:2.3:o:canonical:ubuntu_linux:16.04:*:*:*:esm:*:*:*
cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*:*
cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*:*
cpe:2.3:o:redhat:enterprise_linux_desktop:7.0:*:*:*:*:*:*:*
cpe:2.3:o:redhat:enterprise_linux_desktop:7.0:*:*:*:*:*:*:*
cpe:2.3:o:redhat:enterprise_linux_hpc_node:7.0:*:*:*:*:*:*:*
cpe:2.3:o:redhat:enterprise_linux_hpc_node:7.0:*:*:*:*:*:*:*
cpe:2.3:o:redhat:enterprise_linux_hpc_node_eus:7.2:*:*:*:*:*:*:*
cpe:2.3:o:redhat:enterprise_linux_hpc_node_eus:7.2:*:*:*:*:*:*:*
cpe:2.3:o:redhat:enterprise_linux_server:7.0:*:*:*:*:*:*:*
cpe:2.3:o:redhat:enterprise_linux_server:7.0:*:*:*:*:*:*:*
cpe:2.3:o:redhat:enterprise_linux_server_aus:7.2:*:*:*:*:*:*:*
cpe:2.3:o:redhat:enterprise_linux_server_aus:7.2:*:*:*:*:*:*:*
cpe:2.3:o:redhat:enterprise_linux_server_eus:7.2:*:*:*:*:*:*:*
cpe:2.3:o:redhat:enterprise_linux_server_eus:7.2:*:*:*:*:*:*:*
cpe:2.3:o:redhat:enterprise_linux_workstation:7.0:*:*:*:*:*:*:*
cpe:2.3:o:redhat:enterprise_linux_workstation:7.0:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→