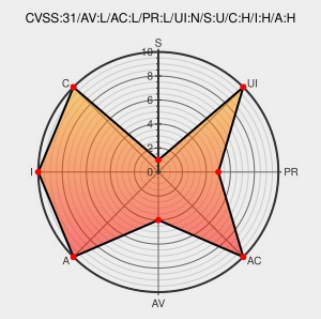
CVE-2014-9322

Published on: 12/17/2014 12:00:00 AM UTC

Last Modified on: 01/17/2023 09:29:00 PM UTC

CVE-2014-9322

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



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

arch/x86/kernel/entry_64.S in the Linux kernel before 3.17.5 does not properly handle faults associated with the Stack Segment (SS) segment register, which allows local users to gain privileges by triggering an IRET instruction that leads to access to a GS Base address from the wrong space.

CVE-2014-9322 has been assigned by cve@mitre.org 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-2015:0812-1: important: Security update for	Mailing List, Third Party Advisory, lists.opensuse.org	SUSE SUSE-SU-2015:0812

	text/html	
Bug 1172806 – CVE-2014-9322 kernel: x86: local privesc due to bad_iret and paranoid entry incompatibility	Issue Tracking Patch Third Party Advisory bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=1172806
oss-security - Linux kernel: multiple x86_64 vulnerabilities	Mailing List Patch Third Party Advisory www.openwall.com text/html	MLIST [oss-security] 20141215 Linux kernel: multiple x86_64 vulnerabilities
kernel/git/torvalds/linux.git - Linux kernel source tree	Mailing List Patch Vendor Advisory git.kernel.org text/html	CONFIRM git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=6f442be2fb22be02cafa606f1769fa1e6f894441
Red Hat Customer Portal	Third Party Advisory web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2014:2008
Red Hat Customer Portal	Third Party Advisory web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2015:0009
Nexus Security Bulletin—April 2016 | Android Open Source Project	Patch Third Party Advisory source.android.com text/html	CONFIRM source.android.com/security/bulletin/2016-04-02.html
Zero Day Initiative	Third Party Advisory VDB Entry www.zerodayinitiative.com text/html	MISC www.zerodayinitiative.com/advisories/ZDI-16-170
'[security bulletin] HPSBGN03285 rev.1 - HP Business Service Manager Virtual Appliance, Multiple Vul' - MARC	Mailing List Third Party Advisory marc.info text/html	HP HPSBGN03285
Red Hat Customer Portal	Third Party Advisory web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2014:2031
No Description Provided	Broken Link osvdb.org Inactive Link Not Archived	OSVDB 115919
USN-2491-1: Linux kernel (EC2) vulnerabilities | Ubuntu	Third Party Advisory www.ubuntu.com text/html	UBUNTU USN-2491-1
[security-announce] SUSE-SU-2015:0736-1: important: Security update for	Mailing List Third Party Advisory lists.opensuse.org text/html	SUSE SUSE-SU-2015:0736
'[security bulletin] HPSBGN03282 rev.1 - HP Business Service Manager	Mailing List Third Party Advisory marc.info	HP HPSBGN03282

Virtual Appliance, Multiple Vuln' - MARC	text/html	
Security Advisory: ZDI-CAN-3263, ZDI-CAN-3284 and ZDI-CAN-3364 Vulnerabilities – Joyent Support	Permissions Required Third Party Advisory help.joyent.com text/html	CONFIRM help.joyent.com/entries/98788667-Security-Advisory-ZDI-CAN-3263-ZDI-CAN-3284-and-ZDI-CAN-3364-Vulnerabilities
[security-announce] openSUSE-SU-2015:0566-1: important: kernel update fo	Mailing List Third Party Advisory lists.opensuse.org text/html	SUSE openSUSE-SU-2015:0566
Linux Kernel IRET Instruction #SS Fault Handling - Crash PoC	Exploit Third Party Advisory VDB Entry www.exploit-db.com Proof of Concept text/html	EXPLOIT-DB 36266
x86_64, traps: Stop using IST for #SS · torvalds/linux@6f442be · GitHub	Patch Third Party Advisory github.com text/html	CONFIRM github.com/torvalds/linux/commit/6f442be2fb22be02cafa606f1769fa1e6f894441
	Mailing List Patch Vendor Advisory www.kernel.org text/plain	CONFIRM www.kernel.org/pub/linux/kernel/v3.x/ChangeLog-3.17.5
Security Advisory SA62336 - Ubuntu update for kernel - Secunia	Broken Link web.archive.org text/html	SECUNIA 62336
Red Hat Customer Portal	Third Party Advisory web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2014:1998
Red Hat Customer Portal	Third Party Advisory web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2014:2028

There are currently no QIDs associated with this CVE

Exploit/POC from Github

CVE-2014-9322 (a.k.a BadIRET) proof of concept for Linux

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating	Canonical	Ubuntu Linux	10.04	All	All	All

System

Operating System	Canonical	Ubuntu Linux	10.04	All	All	All
Operating System	Google	Android	6.0	All	All	All
Operating System	Google	Android	6.0.1	All	All	All
Operating System	Google	Android	6.0	All	All	All
Operating System	Google	Android	6.0.1	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Opensuse	Evergreen	11.4	All	All	All
Operating System	Opensuse	Evergreen	11.4	All	All	All
Operating System	Redhat	Enterprise Linux Eus	5.6	All	All	All
Operating System	Redhat	Enterprise Linux Eus	5.6	All	All	All
Operating System	Suse	Suse Linux Enterprise Server	10	sp4	All	All
Operating System	Suse	Suse Linux Enterprise Server	10	sp4	All	All

cpe:2.3:o:canonical:ubuntu_linux:10.04:*:*:*:-:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:10.04:*:*:*:-:*:*:*:

cpe:2.3:o:google:android:6.0:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:6.0.1:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:6.0:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:6.0.1:*:*:*:*:*:*:*:

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

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

cpe:2.3:o:opensuse:evergreen:11.4:*:*:*:*:*:*:*:

cpe:2.3:o:opensuse:evergreen:11.4:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_eus:5.6:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_eus:5.6:*:*:*:*:*:*:*:

cpe:2.3:o:suse:suse_linux_enterprise_server:10:sp4:*:*:ltss:*:*:*:

cpe:2.3:o:suse:suse_linux_enterprise_server:10:sp4:*:*:ltss:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→