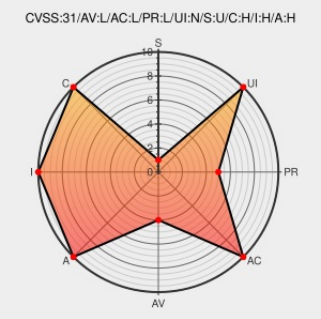
CVE-2018-9568

Published on: 12/06/2018 12:00:00 AM UTC

Last Modified on: 02/24/2023 06:43:00 PM UTC

CVE-2018-9568

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



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

In sk_clone_lock of sock.c, there is a possible memory corruption due to type confusion. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android. Versions: Android kernel. Android ID: A-113509306. References: Upstream kernel.

CVE-2018-9568 has been assigned by security@android.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Google Inc.** - **Android** version **Android kernel**

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
Red Hat Customer Portal	access.redhat.com	REDHAT RHSA-2019:2730

	text/html	
Red Hat Customer Portal	Third Party Advisory access.redhat.com text/html	REDHAT RHSA-2019:0514
USN-3880-1: Linux kernel vulnerabilities | Ubuntu security notices | Ubuntu	Third Party Advisory usn.ubuntu.com text/html	UBUNTU USN-3880-1
Android Security Bulletin—December 2018 | Android Open Source Project	Patch Vendor Advisory source.android.com text/html	CONFIRM source.android.com/security/bulletin/2018-12-01
USN-3880-2: Linux kernel (Trusty HWE) vulnerabilities | Ubuntu security notices	Third Party Advisory usn.ubuntu.com text/html	UBUNTU USN-3880-2
Red Hat Customer Portal	access.redhat.com text/html	REDHAT RHSA-2019:4164
Red Hat Customer Portal	access.redhat.com text/html	REDHAT RHSA-2019:4159
Red Hat Customer Portal	access.redhat.com text/html	REDHAT RHSA-2019:2736
Red Hat Customer Portal	Third Party Advisory access.redhat.com text/html	REDHAT RHSA-2019:0512
Red Hat Customer Portal	access.redhat.com text/html	REDHAT RHSA-2019:4056
Red Hat Customer Portal	access.redhat.com text/html	REDHAT RHSA-2019:4255
Red Hat Customer Portal	access.redhat.com text/html	REDHAT RHSA-2019:3967
Red Hat Customer Portal	access.redhat.com text/html	REDHAT RHSA-2019:2696

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	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating	Canonical	Ubuntu Linux	14.04	All	All	All

Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Google	Android	-	All	All	All
Operating System	Google	Android	-	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 Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.6	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:12.04:*:*:*:esm:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:14.04:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:12.04:*:*:*:esm:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:14.04:*:*:*:lts:*:*:*:

cpe:2.3:o:google:android:-:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:-:*:*:*:*:*:*:*:

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_server:7.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server:7.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server_aus:7.6:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server_aus:7.6:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server_eus:7.6:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server_eus:7.6:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server_tus:7.6:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server_tus:7.6:*:*:*:*:*:*:*:

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→