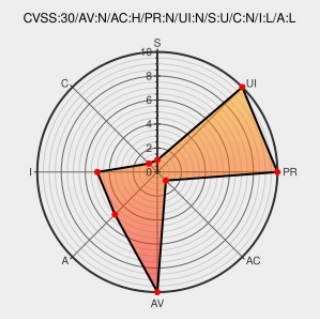
CVE-2016-5696

Published on: 08/06/2016 12:00:00 AM UTC

Last Modified on: 11/17/2021 10:15:00 PM UTC

CVE-2016-5696

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



Certain versions of Android from Google contain the following vulnerability:

net/ipv4/tcp_input.c in the Linux kernel before 4.7 does not properly determine the rate of challenge ACK segments, which makes it easier for remote attackers to hijack TCP sessions via a blind in-window attack.

CVE-2016-5696 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 4.8 - MEDIUM

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

CVSS2 Score: 5.8 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
CVE-2016-5696 Kernel Vulnerability	security.paloaltonetworks.com text/html	CONFIRM security.paloaltonetworks.com/CVE-2016-5696
Bug 1354708 – CVE-2016-5696 kernel:	Issue Tracking bugzilla.redhat.com	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=1354708

challenge ACK counter information disclosure.	text/html	
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2016:1814
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2016:1632
USN-3070-2: Linux kernel (Raspberry Pi 2) vulnerabilities | Ubuntu	www.ubuntu.com text/html	UBUNTU USN-3070-2
oss-security - Re: CVE-2016-5389: linux kernel - challange ack information leak.	Mailing List Third Party Advisory www.openwall.com text/html	MLIST [oss-security] 20160712 Re: CVE-2016-5389: linux kernel - challange ack information leak.
tcp: make challenge acks less predictable · torvalds/linux@75ff39c · GitHub	Issue Tracking Patch github.com text/html	CONFIRM github.com/torvalds/linux/commit/75ff39ccc1bd5d3c455b6822ab09e533c551f758
Oracle Linux Bulletin - July 2016	Third Party Advisory web.archive.org text/html Inactive Link Not Archived	CONFIRM www.oracle.com/technetwork/topics/security/linuxbulletinjul2016-3090544.html
Security Advisory 0023 - Arista	www.arista.com text/html	MISC www.arista.com/en/support/advisories-notices/security-advisories/1461-security-advisory-23
Mitnick Attack Reappears at GeekPwn Macau Contest	Technical Description www.prnewswire.com text/html	MISC www.prnewswire.com/news-releases/mitnick-attack-reappears-at-geekpwn-macau-contest-300270779.html
	Technical Description www.usenix.org application/pdf	MISC www.usenix.org/system/files/conference/usenixsecurity16/sec16_paper_cao.pdf
GitHub - Gnoxter/mountain_goat: A PoC demonstrating techniques exploiting CVE-2016-5696 Off-Path TCP Exploits: Global Rate Limit Considered Dangerous	Exploit Third Party Advisory github.com text/html	MISC github.com/Gnoxter/mountain_goat
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2016:1657
USN-3070-4: Linux kernel (Xenial HWE) vulnerabilities | Ubuntu	www.ubuntu.com text/html	UBUNTU USN-3070-4
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2016:1939
USN-3072-1: Linux kernel vulnerabilities | Ubuntu	www.ubuntu.com text/html	UBUNTU USN-3072-1
USN-3071-2: Linux kernel (Trusty HWE) vulnerabilities | Ubuntu	www.ubuntu.com text/html	UBUNTU USN-3071-2

Broadcom Support Portal	bto.bluecoat.com text/html	CONFIRM bto.bluecoat.com/security-advisory/sa131
Oracle VM Server for x86 Bulletin - July 2016	Vendor Advisory web.archive.org text/html Inactive Link Not Archived	CONFIRM www.oracle.com/technetwork/topics/security/ovmbulletinjul2016-3090546.html
Android Security Bulletin—October 2016 | Android Open Source Project	Third Party Advisory source.android.com text/html	CONFIRM source.android.com/security/bulletin/2016-10-01.html
USN-3072-2: Linux kernel (OMAP4) vulnerabilities | Ubuntu	www.ubuntu.com text/html	UBUNTU USN-3072-2
USN-3071-1: Linux kernel vulnerabilities | Ubuntu	www.ubuntu.com text/html	UBUNTU USN-3071-1
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2016:1664
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2016:1631
McAfee Security Bulletin: kernel challenge ACK counter information disclosure vulnerability (CVE-2016-5696)	kc.mcafee.com text/html	CONFIRM kc.mcafee.com/corporate/index?page=content&id=SB10167
Linux Kernel 'Ack Challenge' Information Disclosure Vulnerability	cve.report (archive) text/html	BID 91704
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2016:1815
kernel/git/torvalds/linux.git - Linux kernel source tree	Issue Tracking Patch git.kernel.org text/html	CONFIRM git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=75ff39ccc1bd5d3c455b6822ab09e533c551f758
USN-3070-1: Linux kernel vulnerabilities | Ubuntu	www.ubuntu.com text/html	UBUNTU USN-3070-1
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2016:1633
USN-3070-3: Linux kernel (Qualcomm Snapdragon) vulnerabilities | Ubuntu	www.ubuntu.com text/html	UBUNTU USN-3070-3
Linux Kernel Lets Remote Users Obtain Potentially Sensitive Information About, Deny Service, and Hijack Target TCP Connections in Certain Cases - SecurityTracker	www.securitytracker.com text/html	SECTRACK 1036625

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

Exploit/POC from Github

Daemon to randomize tcp_challenge_ack_limit to prevent side channel attacks CVE-2016-5696

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Google	Android	All	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Application	Oracle	Vm Server	3.3	All	All	All
Application	Oracle	Vm Server	3.4	All	All	All
Application	Oracle	Vm Server	3.3	All	All	All
Application	Oracle	Vm Server	3.4	All	All	All

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

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

cpe:2.3:a:oracle:vm_server:3.3:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:vm_server:3.4:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:vm_server:3.3:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:vm_server:3.4:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→