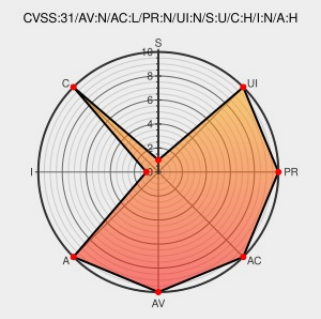
CVE-2014-3180

Published on: 11/06/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:46 PM UTC

CVE-2014-3180

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



Certain versions of Chrome Os from Google contain the following vulnerability:

** DISPUTED ** In kernel/compat.c in the Linux kernel before 3.17, as used in Google Chrome OS and other products, there is a possible out-of-bounds read. restart_syscall uses uninitialized data when restarting compat_sys_nanosleep. NOTE: this is disputed because the code path is unreachable.

CVE-2014-3180 has been assigned by security@google.com to track the vulnerability - currently rated as CRITICAL severity.

Affected Vendor/Software: **Linux** - **kernel** version **before 3.17**

CVSS3 Score: 9.1 - CRITICAL

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

CVSS2 Score: 6.4 - MEDIUM

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

CVE References

Description	Tags	Link
LKML: Thomas Gleixner: [GIT pull] timer updates for 3.17	Patch	MISC lkml.org/lkml/2014/9/7/29

	Third Party Advisory lkml.org text/xml	
Issue 408827 - chromium - restart_syscall uses uninitialized data when restarting compat_sys_nanosleep - Monorail	Third Party Advisory bugs.chromium.org text/html	MISC bugs.chromium.org/p/chromium/issues/detail?id=408827

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	Google	Chrome Os	-	All	All	All
Operating System	Google	Chrome Os	-	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All

cpe:2.3:o:google:chrome_os:-:*:*:*:*:*:*:*:

cpe:2.3:o:google:chrome_os:-:*:*:*:*:*:*:*:

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→