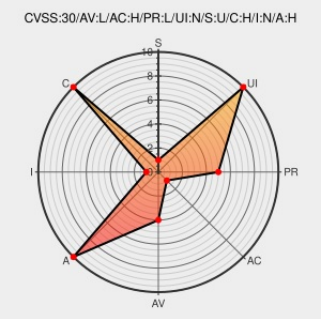
CVE-2018-12633

Published on: 06/21/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:23 PM UTC

CVE-2018-12633

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



Certain versions of Linux Kernel from Linux contain the following vulnerability:

An issue was discovered in the Linux kernel through 4.17.2. vbg_misc_device_ioctl() in drivers/virt/vboxguest/vboxguest_linux.c reads the same user data twice with copy_from_user. The header part of the user data is double-fetched, and a malicious user thread can tamper with the critical variables (hdr.size_in and hdr.size_out) in the header between the two fetches because of a race condition, leading to severe kernel errors, such as buffer over-accesses. This bug can cause a local denial of service and information leakage.

CVE-2018-12633 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 6.3 - MEDIUM

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

CVSS2 Score: 6.3 - MEDIUM

Access Vector	Access Complexity	Authentication
LOCAL	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	NONE	COMPLETE

CVE References

Description	Tags	Link

kernel/git/torvalds/linux.git - Linux kernel source tree	Patch Vendor Advisory git.kernel.org text/html	MISC git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=bd23a7269834dc7c1f93e83535d16ebc44b75eba
virt: vbox: Only copy_from_user the request-header once · torvalds/linux@bd23a72 · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/torvalds/linux/commit/bd23a7269834dc7c1f93e83535d16e
200131 – Double-Fetch bug in Linux-4.16.8/drivers/virt/vboxguest/vboxguest_linux.c.	Issue Tracking Vendor Advisory bugzilla.kernel.org text/html	MISC bugzilla.kernel.org/show_bug.cgi?id=200131

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	All	All	All	All

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→