CVE-2018-14656

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2018-14656
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-10-08 22:29:00 UTC
Updated	2023-02-13 04:51:00 UTC
Description	A missing address check in the callers of the show_opcodes() in the Linux kernel allows an attacker to dump the kernel mer

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	4.19	rc1	All	All
Operating System	Linux	Linux Kernel	4.19	rc1	All	All
Operating System	Linux	Linux Kernel	All	All	All	All

References

Reference
1629940 – (CVE-2018-14656) CVE-2018-14656 kernel: Arbitrary Kernel Read into dmesg via Missing Address Check in segfault Handler
oss-sec: CVE-2018-14656: Linux kernel: arbitrary kernel memory dump into the dmesg log
[PATCH v2] x86/dumpstack: don't dump kernel memory based on usermode RIP
Issue 1650 - project-zero - Project Zero - Monorail
Linux Kernel Missing Address Validation in show_opcodes() Lets Local Users Obtain Potentially Sensitive Information on the Target System -
kernel/git/torvalds/linux.git - Linux kernel source tree
[PATCH v2] x86/dumpstack: don't dump kernel memory based on usermode RIP
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**