CVE-2017-7518

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

Summary

CVE	CVE-2017-7518
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-07-30 15:29:00 UTC
Updated	2023-11-07 02:50:00 UTC
Description	A flaw was found in the Linux kernel before version 4.12 in the way the KVM module processed the trap flag(TF) bit in EFL

Risk And Classification

Problem Types: CWE-755

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	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	7.4	All	All	All

Operating System	Redhat	Enterprise Linux Server Aus	7.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.5	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.5	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

References

Reference
Linux Kernel CVE-2017-7518 Privilage Escalation Vulnerability
CVE-2017-7518 Kernel: KVM: debug exception via syscall emulation - Red Hat Customer Portal
USN-3619-1: Linux kernel vulnerabilities | Ubuntu security notices
USN-3619-2: Linux kernel (Xenial HWE) vulnerabilities | Ubuntu security notices
[PATCH] KVM: x86: fix singlestepping over syscall — Linux KVM
oss-security - CVE-2017-7518 Kernel: KVM: debug exception via syscall emulation
Debian -- Security Information -- DSA-3981-1 linux
Red Hat Customer Portal
1464473 – (CVE-2017-7518) CVE-2017-7518 Kernel: KVM: debug exception via syscall emulation
USN-3754-1: Linux kernel vulnerabilities | Ubuntu security notices | Ubuntu
Red Hat Customer Portal
KVM Syscall Emulation Debug Error Lets Local Users on a Guest System Gain Elevated Privileges on the Guest System - SecurityTracker
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.

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