



CVE-2018-10853

Published on: 09/11/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:20 PM UTC

CVE-2018-10853

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Ubuntu Linux](#) from [Canonical](#) contain the following vulnerability:

A flaw was found in the way Linux kernel KVM hypervisor before 4.18 emulated instructions such as sgdt/sidt/fxsave/fxrstor. It did not check current privilege(CPL) level while emulating unprivileged instructions. An unprivileged guest user/process could use this flaw to potentially escalate privileges inside guest.

CVE-2018-10853 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: **Linux - kernel version 4.18**

CVSS3 Score: **7.8 - HIGH**

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

CVSS2 Score: **4.6 - MEDIUM**

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
[security-announce] openSUSE-SU-2019:1407-1:	lists.opensuse.org	SUSE openSUSE-SU-2019:1407

important: Security update	text/html	
Red Hat Customer Portal	access.redhat.com text/html	 REDHAT RHSA-2019:2029
kernel/git/torvalds/linux.git - Linux kernel source tree	Patch Vendor Advisory git.kernel.org text/html	 CONFIRM git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=3c9fa24ca7c9c47605672916491f79e8ccacb9e6
[SECURITY] [DLA 1422-1] linux security update	Mailing List Third Party Advisory lists.debian.org text/html	 MLIST [debian-lts-announce] 20180714 [SECURITY] [DLA 1422-1] linux security update
Red Hat Customer Portal	access.redhat.com text/html	 REDHAT RHSA-2019:2043
[SECURITY] [DLA 1423-1] linux-4.9 new package	Mailing List Third Party Advisory lists.debian.org text/html	 MLIST [debian-lts-announce] 20180718 [SECURITY] [DLA 1423-1] linux-4.9 new package
[SECURITY] [DLA 1422-2] linux security update	Mailing List Third Party Advisory lists.debian.org text/html	 MLIST [debian-lts-announce] 20180715 [SECURITY] [DLA 1422-2] linux security update
1589890 – (CVE-2018-10853) CVE-2018-10853 kernel: kvm: guest userspace to guest kernel write	Issue Tracking Patch Third Party Advisory bugzilla.redhat.com text/html	 CONFIRM bugzilla.redhat.com/show_bug.cgi?id=CVE-2018-10853
USN-3777-2: Linux kernel (HWE) vulnerabilities Ubuntu security notices	Third Party Advisory usn.ubuntu.com text/html	 UBUNTU USN-3777-2
USN-3777-1: Linux kernel vulnerabilities Ubuntu security notices	Third Party Advisory usn.ubuntu.com text/html	 UBUNTU USN-3777-1
Red Hat Customer Portal	access.redhat.com text/html	 REDHAT RHSA-2020:0179
kernel/git/torvalds/linux.git - Linux kernel source tree	Patch Vendor Advisory git.kernel.org text/html	 CONFIRM git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=129a72a0d3c8e139a04512325384fe5ac119e74
oss-security - CVE-2018-10853 kernel: kvm: guest userspace to guest kernel write	Mailing List Patch Third Party Advisory www.openwall.com text/html	 MISC www.openwall.com/lists/oss-security/2018/09/02/1
Red Hat Customer Portal	access.redhat.com text/html	 REDHAT RHSA-2020:0036
Red Hat Customer Portal	access.redhat.com text/html	 REDHAT RHSA-2020:0103

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	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	8.0	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:canonical:ubuntu_linux:16.04:*:*:*:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:18.04:*:*:*:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:16.04:*:*:*:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:18.04:*:*:*:*:*:						
cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*:*:						
cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*:*:						
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 →](#)

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)