



CVE-2018-5750

Published on: 01/26/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:45 PM UTC

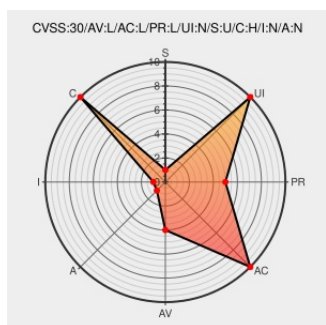
CVE-2018-5750

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



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

The `acpi_smbus_hc_add` function in `drivers/acpi/sbshc.c` in the Linux kernel through 4.14.15 allows local users to obtain sensitive address information by reading `dmesg` data from an SBS HC `printk` call.

CVE-2018-5750 has been assigned by [M](#) `cve@mitre.org` to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **5.5 - MEDIUM**

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

CVSS2 Score: **2.1 - LOW**

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

CVE References

Description	Tags	Link
USN-3631-2: Linux kernel (Xenial HWE) vulnerabilities Ubuntu security notices	Third Party Advisory usn.ubuntu.com text/html	UBUNTU USN-3631-2
USN-3698-1: Linux kernel vulnerabilities Ubuntu security notices	Third Party Advisory	UBUNTU USN-3698-1

[usn.ubuntu.com](#)
[text/html](#)

USN-3631-1: Linux kernel vulnerabilities | Ubuntu security notices

[Third Party Advisory](#)
[usn.ubuntu.com](#)
[text/html](#)

 [UBUNTU USN-3631-1](#)

USN-3698-2: Linux kernel (Trusty HWE) vulnerabilities | Ubuntu security notices

[Third Party Advisory](#)
[usn.ubuntu.com](#)
[text/html](#)

 [UBUNTU USN-3698-2](#)

Red Hat Customer Portal

[Third Party Advisory](#)
[access.redhat.com](#)
[text/html](#)

 [REDHAT RHSA-2018:0676](#)

ACPI: sbshc: remove raw pointer from printk message - Patchwork

[Issue Tracking](#)
[Patch](#)
[Third Party Advisory](#)
[patchwork.kernel.org](#)
[text/html](#)

 [CONFIRM](#)
[patchwork.kernel.org/patch/10174835/](#)

Debian -- Security Information -- DSA-4187-1 linux

[Third Party Advisory](#)
[www.debian.org](#)
[Deprecated Link](#)
[text/html](#)

 [DEBIAN DSA-4187](#)

[SECURITY] [DLA 1369-1] linux security update

[Mailing List](#)
[Third Party Advisory](#)
[lists.debian.org](#)
[text/html](#)

 [MLIST \[debian-lts-announce\]](#)
[20180502 \[SECURITY\] \[DLA 1369-1\]](#)
[linux security update](#)

Red Hat Customer Portal

[Third Party Advisory](#)
[access.redhat.com](#)
[text/html](#)

 [REDHAT RHSA-2018:1062](#)

USN-3697-2: Linux kernel (OEM) vulnerabilities | Ubuntu security notices

[Third Party Advisory](#)
[usn.ubuntu.com](#)
[text/html](#)

 [UBUNTU USN-3697-2](#)

Debian -- Security Information -- DSA-4120-1 linux

[Third Party Advisory](#)
[www.debian.org](#)
[Deprecated Link](#)
[text/html](#)

 [DEBIAN DSA-4120](#)

Red Hat Customer Portal

[Third Party Advisory](#)
[access.redhat.com](#)
[text/html](#)

 [REDHAT RHSA-2018:2948](#)

USN-3697-1: Linux kernel vulnerabilities | Ubuntu security notices

[Third Party Advisory](#)
[usn.ubuntu.com](#)
[text/html](#)

 [UBUNTU USN-3697-1](#)

Linux Kernel ACPI Driver Bug Lets Local Users Obtain Potentially Sensitive Information and Bypass ASLR - SecurityTracker

[Third Party Advisory](#)
[VDB Entry](#)
[www.securitytracker.com](#)
[text/html](#)

 [SECTrack 1040319](#)

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	12.04	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	Canonical	Ubuntu Linux	17.10	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	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	Canonical	Ubuntu Linux	17.10	All	All	All
Operating System	Debian	Debian Linux	7.0	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	Debian	Debian Linux	7.0	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	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	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.6	All	All	All

System

Operating System	Redhat	Enterprise Linux Server Eus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.6	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
Application	Redhat	Virtualization Host	4.0	All	All	All
Application	Redhat	Virtualization Host	4.0	All	All	All
cpe:2.3:o:canonical:ubuntu_linux:12.04:*:*:*:esm:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:14.04:*:*:*:lts:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:16.04:*:*:*:lts:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:17.10:*:*:*:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:12.04:*:*:*:esm:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:14.04:*:*:*:lts:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:16.04:*:*:*:lts:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:17.10:*:*:*:*:*:						
cpe:2.3:o:debian:debian_linux:7.0:*:*:*:*:*:						
cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*:*:						
cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*:*:						
cpe:2.3:o:debian:debian_linux:7.0:*:*:*:*:*:						
cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*:*:						
cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*:*:						
cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:						
cpe:2.3:o:redhat:enterprise_linux_desktop:7.0:*:*:*:*:*:						
cpe:2.3:o:redhat:enterprise_linux_desktop:7.0:*:*:*:*:*:						
cpe:2.3:o:redhat:enterprise_linux_server:7.0:*:*:*:*:*:						
cpe:2.3:o:redhat:enterprise_linux_server:7.0:*:*:*:*:*:						
cpe:2.3:o:redhat:enterprise_linux_server_aus:7.6:*:*:*:*:*:						

cpe:2.3:o:redhat:enterprise_linux_server_aus:7.6:*:*:*:*:*:
cpe:2.3:o:redhat:enterprise_linux_server_eus:7.6:*:*:*:*:*:
cpe:2.3:o:redhat:enterprise_linux_server_eus:7.6:*:*:*:*:*:
cpe:2.3:o:redhat:enterprise_linux_server_tus:7.6:*:*:*:*:*:
cpe:2.3:o:redhat:enterprise_linux_server_tus:7.6:*:*:*:*:*:
cpe:2.3:o:redhat:enterprise_linux_workstation:7.0:*:*:*:*:*:
cpe:2.3:o:redhat:enterprise_linux_workstation:7.0:*:*:*:*:*:
cpe:2.3:a:redhat:virtualization_host:4.0:*:*:*:*:*:
cpe:2.3:a:redhat:virtualization_host:4.0:*:*:*:*:*:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

© [CVE.report](#) 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

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](#)