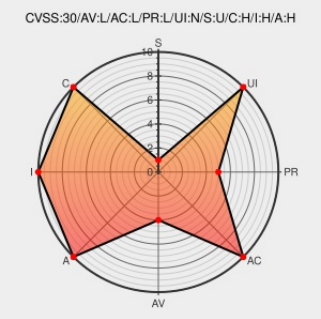
CVE-2018-5848

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

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

CVE-2018-5848

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



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

In the function wmi_set_ie(), the length validation code does not handle unsigned integer overflow properly. As a result, a large value of the 'ie_len' argument can cause a buffer overflow in all Android releases from CAF (Android for MSM, Firefox OS for MSM, QRD Android) using the Linux Kernel.

CVE-2018-5848 has been assigned by product-security@qualcomm.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Qualcomm, Inc.** - **Android for MSM, Firefox OS for MSM, QRD Android** version **All Android releases from CAF using the Linux kernel**

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] [DLA 1715-1] linux-4.9 security update	Mailing List Third Party Advisory lists.debian.org text/html	MLIST [debian-lts-announce] 20190315 [SECURITY] [DLA 1715-1] linux-4.9 security update
[SECURITY] [DLA 1731-2] linux regression update	Mailing List Third Party Advisory lists.debian.org text/html	MLIST [debian-lts-announce] 20190401 [SECURITY] [DLA 1731-2] linux regression update
Pixel/Nexus Security Bulletin—May 2018	Vendor Advisory source.android.com text/html	MISC MISC
Red Hat Customer Portal	Third Party Advisory access.redhat.com text/html	REDHAT RHSA-2018:3083
May 2018 Code Aurora Security Bulletin - Code Aurora	Patch Third Party Advisory www.codeaurora.org text/html	MISC www.codeaurora.org/security-bulletin/2018/05/11/may-2018-code-aurora-security-bulletin-2
[SECURITY] [DLA 1731-1] linux security update	Mailing List Third Party Advisory lists.debian.org text/html	MLIST [debian-lts-announce] 20190327 [SECURITY] [DLA 1731-1] linux security update
Red Hat Customer Portal	Third Party Advisory access.redhat.com text/html	REDHAT RHSA-2018:2948
Red Hat Customer Portal	Third Party Advisory access.redhat.com text/html	REDHAT RHSA-2018:3096

Related QID Numbers

753730 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 20 for SLE 12 SP2) (SUSE-SU-2018:4127-1)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Google	Android	-	All	All	All
Operating System	Google	Android	-	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating	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 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:debian:debian_linux:8.0:*:*:*:*:*:*:*:
- cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*:*:*:*:
- cpe:2.3:o:google:android:-:*:*:*:*:*:*:*:
- cpe:2.3:o:google:android:-:*:*:*:*:*:*:*:
- 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_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→