ROYAUME DU MAROC
ADMINISTRATION
DE LA DEFENSE NATIONALE
Direction Générale de la Sécurité
des Systèmes d'Information

المملكة المغربية
إدارة الدفاع الوطني
المديرية العامة لأمن نظم المعلومات
مديرية تدبير مركز اليقظة والرصد
والتصدي للهجمات المعلوماتية

**BULLETIN DE SECURITE**

# Titre: Vulnérabilités dans le noyau Linux

**Numéro de Référence : 20841806/19**

**Risque : Important**
**Impact : Important**

**Systèmes affectés**

- Debian versions antérieures à 4.9.168-1+deb9u3
- Ubuntu 19.04
- Ubuntu 18.10
- Ubuntu 18.04 LTS
- Ubuntu 16.04 LTS
- Ubuntu 14.04 ESM
- Ubuntu 12.04 ESM
- Red Hat CodeReady Linux Builder pour ARM 64 8 aarch64
- Red Hat CodeReady Linux Builder pour Power, little endian 8 ppc64le
- Red Hat CodeReady Linux Builder pour x86_64 8 x86_64
- Red Hat Enterprise Linux Desktop 6 i386
- Red Hat Enterprise Linux Desktop 6 x86_64
- Red Hat Enterprise Linux Desktop 7 x86_64
- Red Hat Enterprise Linux EUS Compute Node 7.4 x86_64
- Red Hat Enterprise Linux EUS Compute Node 7.6 x86_64
- Red Hat Enterprise Linux pour ARM 64 8 aarch64
- Red Hat Enterprise Linux pour IBM z Systems 6 s390x
- Red Hat Enterprise Linux pour IBM z Systems 7 s390x
- Red Hat Enterprise Linux pour IBM z Systems 8 s390x
- Red Hat Enterprise Linux pour IBM z Systems - Extended Update Support 7.4 s390x
- Red Hat Enterprise Linux pour IBM z Systems - Extended Update Support 7.6 s390x
- Red Hat Enterprise Linux pour Power, big endian 6 ppc64
- Red Hat Enterprise Linux pour Power, big endian 7 ppc64
- Red Hat Enterprise Linux pour Power, big endian - Extended Update Support 7.4 ppc64
- Red Hat Enterprise Linux pour Power, big endian - Extended Update Support 7.6 ppc64
- Red Hat Enterprise Linux pour Power, little endian 7 ppc64le
- Red Hat Enterprise Linux pour Power, little endian 8 ppc64le

- Red Hat Enterprise Linux pour Power, little endian - Extended Update Support 7.4 ppc64le
- Red Hat Enterprise Linux pour Power, little endian - Extended Update Support 7.6 ppc64le
- Red Hat Enterprise Linux pour Real Time 7 x86_64
- Red Hat Enterprise Linux pour Real Time 8 x86_64
- Red Hat Enterprise Linux pour Real Time pour NFV 7 x86_64
- Red Hat Enterprise Linux pour Real Time pour NFV 8 x86_64
- Red Hat Enterprise Linux pour Scientific Computing 6 x86_64
- Red Hat Enterprise Linux pour Scientific Computing 7 x86_64
- Red Hat Enterprise Linux pour x86_64 8 x86_64
- Red Hat Enterprise Linux Server 6 i386
- Red Hat Enterprise Linux Server 6 x86_64
- Red Hat Enterprise Linux Server 7 x86_64
- Red Hat Enterprise Linux Server versions AUS 6.5 x86_64, AUS 6.6 x86_64, AUS 7.2 x86_64, AUS 7.3 x86_64, AUS 7.4 x86_64, AUS 7.6 x86_64
- Red Hat Enterprise Linux Server - Extended Update Support 7.4 x86_64
- Red Hat Enterprise Linux Server - Extended Update Support 7.6 x86_64
- Red Hat Enterprise Linux Server (pour IBM Power LE) - Update Services pour SAP Solutions 7.3 ppc64le
- Red Hat Enterprise Linux Server (pour IBM Power LE) - Update Services pour SAP Solutions 7.4 ppc64le
- Red Hat Enterprise Linux Server (pour IBM Power LE) - Update Services pour SAP Solutions 7.6 ppc64le
- Red Hat Enterprise Linux Server versions TUS 7.2 x86_64, TUS 7.3 x86_64, TUS 7.4 x86_64, TUS 7.6 x86_64
- Red Hat Enterprise Linux Server - Update Services pour SAP Solutions 7.2 x86_64
- Red Hat Enterprise Linux Server - Update Services pour SAP Solutions 7.3 x86_64
- Red Hat Enterprise Linux Server - Update Services pour SAP Solutions 7.4 x86_64
- Red Hat Enterprise Linux Server - Update Services pour SAP Solutions 7.6 x86_64
- Red Hat Enterprise Linux Workstation 6 i386
- Red Hat Enterprise Linux Workstation 6 x86_64
- Red Hat Enterprise Linux Workstation 7 x86_64
- Red Hat Virtualization Host 4 x86_64
- Red Hat Virtualization Host - Extended Update Support 4.2 x86_64

## Identificateurs externes

- CVE-2019-3846 CVE-2019-10126 CVE-2019-5489 CVE-2019-9500 CVE-2019-9503
- CVE-2019-11477 CVE-2019-11478 CVE-2019-11479 CVE-2019-11486 CVE-2019-11599
- CVE-2019-11815 CVE-2019-11833 CVE-2019-11884

### Bilan de la vulnérabilité

Plusieurs vulnérabilités ont été corrigées dans le noyau Linux des distributions Ubuntu, Debian et Red Hat. Un attaquant pourrait exploiter ces vulnérabilités afin de provoquer une exécution de code arbitraire à distance, un déni de service à distance et une élévation de privilèges.

**Solution**

Veuillez-vous référer aux bulletins de sécurité des distributions linux Debien, Ubuntu et Red Hat du 17 Juin 2019.

**Risque :**

- Exécution de code arbitraire à distance
- Déni de service à distance
- Élévation de privilèges

**Annexe**

Bulletin de sécurité Debian DSA-4465-1 du 17 juin 2019 :
https://www.debian.org/security/2019/dsa-4465

Bulletin de sécurité Ubuntu USN-4017-1 du 17 juin 2019 :
https://usn.ubuntu.com/4017-1/

Bulletin de sécurité Ubuntu USN-4017-2 du 17 juin 2019 :
https://usn.ubuntu.com/4017-2/

Bulletin de sécurité RedHat RHSA-2019:1487 du 17 juin 2019

https://access.redhat.com/errata/RHSA-2019:1487

Bulletin de sécurité RedHat RHSA-2019:1486 du 17 juin 2019

https://access.redhat.com/errata/RHSA-2019:1486

Bulletin de sécurité RedHat RHSA-2019:1480 du 17 juin 2019

https://access.redhat.com/errata/RHSA-2019:1480

Bulletin de sécurité RedHat RHSA-2019:1490 du 17 juin 2019

https://access.redhat.com/errata/RHSA-2019:1490

Bulletin de sécurité RedHat RHSA-2019:1489 du 17 juin 2019

https://access.redhat.com/errata/RHSA-2019:1489

Bulletin de sécurité RedHat RHSA-2019:1485 du 17 juin 2019

https://access.redhat.com/errata/RHSA-2019:1485

Bulletin de sécurité RedHat RHSA-2019:1484 du 17 juin 2019

https://access.redhat.com/errata/RHSA-2019:1484

Bulletin de sécurité RedHat RHSA-2019:1483 du 17 juin 2019

https://access.redhat.com/errata/RHSA-2019:1483

Bulletin de sécurité RedHat RHSA-2019:1488 du 17 juin 2019

https://access.redhat.com/errata/RHSA-2019:1488

Bulletin de sécurité RedHat RHSA-2019:1481 du 17 juin 2019

https://access.redhat.com/errata/RHSA-2019:1481

Bulletin de sécurité RedHat RHSA-2019:1479 du 17 juin 2019

https://access.redhat.com/errata/RHSA-2019:1479