

Agence Nationale
des Systèmes d'information
de l'état

Djibouti le, 29-06-2024

BULLETIN ALERTES

Object	Multiples vulnérabilités dans s le noyau Linux de Red Hat
Référence	1177
Date de Publication	2024-06-28
Sévérité	Elevé

IMPACT :

- Atteinte à la confidentialité des données
- Déni de service
- Exécution de code arbitraire à distance
- Élévation de privilèges

SYSTÈME AFFECTÉ :

- Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.2 aarch64
- Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.2 s390x
- Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.2 ppc64le
- Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.2 x86_64
- Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.2 aarch64
- Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.2 s390x
- Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.2 ppc64le
- Red Hat Enterprise Linux for Real Time for NFV for x86_64 - 4 years of updates 9.2 x86_64
- Red Hat Enterprise Linux for Real Time for x86_64 - 4 years of updates 9.2 x86_64
- Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.2 x86_64
- Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.6 x86_64
- Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.2 x86_64
- Red Hat Enterprise Linux Server - AUS 7.6 x86_64
- Red Hat Enterprise Linux Server - AUS 8.6 x86_64
- Red Hat Enterprise Linux Server - AUS 9.2 x86_64
- Red Hat Enterprise Linux Server - TUS 8.6 x86_64
- Red Hat Enterprise Linux Server for ARM 64 - 4 years of updates 9.2 aarch64
- Red Hat Enterprise Linux Server for IBM z Systems - 4 years of updates 9.2 s390x
- Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.6 ppc64le
- Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.2 ppc64le

DÉSCRIPTION :

De multiples vulnérabilités ont été découvertes dans le noyau Linux de Red Hat. Certaines d'entre elles permettent à un attaquant de provoquer une élévation de privilèges, une atteinte à la confidentialité des données et un contournement de la politique de sécurité.

SOLUTION :

Mettre à jour le noyau Linux de Red Hat.(se réfère à la section documentation)

DOCUMENTATION :

- Bulletin de sécurité Red Hat RHSA-2024:4098 du 25 juin 2024

<https://access.redhat.com/errata/RHSA-2024:4098>

- Bulletin de sécurité Red Hat RHSA-2024:4106 du 26 juin 2024

<https://access.redhat.com/errata/RHSA-2024:4106>

- Bulletin de sécurité Red Hat RHSA-2024:4107 du 26 juin 2024

<https://access.redhat.com/errata/RHSA-2024:4107>

- Bulletin de sécurité Red Hat RHSA-2024:4108 du 26 juin 2024

<https://access.redhat.com/errata/RHSA-2024:4108>

- CVE CVE-2021-47400

<https://www.cve.org/CVERecord?id=CVE-2021-47400>

- CVE CVE-2022-1048

<https://www.cve.org/CVERecord?id=CVE-2022-1048>

- CVE CVE-2023-2002

<https://www.cve.org/CVERecord?id=CVE-2023-2002>

- CVE CVE-2024-26642

<https://www.cve.org/CVERecord?id=CVE-2024-26642>

- CVE CVE-2024-26993

<https://www.cve.org/CVERecord?id=CVE-2024-26993>

- CVE CVE-2024-27393

<https://www.cve.org/CVERecord?id=CVE-2024-27393>

- CVE CVE-2024-27397

<https://www.cve.org/CVERecord?id=CVE-2024-27397>

- CVE CVE-2024-27403

<https://www.cve.org/CVERecord?id=CVE-2024-27403>

- CVE CVE-2024-35870

<https://www.cve.org/CVERecord?id=CVE-2024-35870>

- CVE CVE-2024-35958

<https://www.cve.org/CVERecord?id=CVE-2024-35958>

- CVE CVE-2024-35960

<https://www.cve.org/CVERecord?id=CVE-2024-35960>

- CVE CVE-2024-36957

<https://www.cve.org/CVERecord?id=CVE-2024-36957>