

Agence Nationale
des Systèmes d'information
de l'état

Djibouti le, 27-05-2024

BULLETIN ALERTES

Object	Multiples vulnérabilités dans le noyau Linux de Red Hat
Référence	1147
Date de Publication	2024-05-27
Sévérité	Critique

IMPACT :

- Atteinte à l'intégrité des données
- Atteinte à la confidentialité des données
- Contournement de la politique de sécurité
- Déni de service à distance
- Exécution de code arbitraire
- Élévation de privilèges

SYSTÈME AFFECTÉ :

- Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.4 aarch64
- Red Hat CodeReady Linux Builder for ARM 64 8 aarch64
- Red Hat CodeReady Linux Builder for ARM 64 9 aarch64
- Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.4 s390x
- Red Hat CodeReady Linux Builder for IBM z Systems 9 s390x
- Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.4 ppc64le
- Red Hat CodeReady Linux Builder for Power, little endian 8 ppc64le
- Red Hat CodeReady Linux Builder for Power, little endian 9 ppc64le
- Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.4 x86_64
- Red Hat CodeReady Linux Builder for x86_64 8 x86_64

- Red Hat CodeReady Linux Builder for x86_64 9 x86_64
- Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.4 aarch64
- Red Hat Enterprise Linux for ARM 64 8 aarch64
- Red Hat Enterprise Linux for ARM 64 9 aarch64
- Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.4 s390x
- Red Hat Enterprise Linux for IBM z Systems 8 s390x
- Red Hat Enterprise Linux for IBM z Systems 9 s390x
- Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.4 ppc64le
- Red Hat Enterprise Linux for Power, little endian 8 ppc64le
- Red Hat Enterprise Linux for Power, little endian 9 ppc64le
- Red Hat Enterprise Linux for Real Time 8 x86_64
- Red Hat Enterprise Linux for Real Time 9 x86_64
- Red Hat Enterprise Linux for Real Time for NFV 8 x86_64
- Red Hat Enterprise Linux for Real Time for NFV 9 x86_64
- Red Hat Enterprise Linux for Real Time for NFV for x86_64 - 4 years of updates 9.4 x86_64
- Red Hat Enterprise Linux for Real Time for x86_64 - 4 years of updates 9.4 x86_64
- Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.4 x86_64
- Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.4 x86_64
- Red Hat Enterprise Linux for x86_64 8 x86_64
- Red Hat Enterprise Linux for x86_64 9 x86_64
- Red Hat Enterprise Linux Server - AUS 7.6 x86_64
- Red Hat Enterprise Linux Server - AUS 7.7 x86_64
- Red Hat Enterprise Linux Server - AUS 9.4 x86_64
- Red Hat Enterprise Linux Server for ARM 64 - 4 years of updates 9.4 aarch64
- Red Hat Enterprise Linux Server for IBM z Systems - 4 years of updates 9.4 s390x
- Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.4 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 exécution de code arbitraire, une élévation de privilèges et un déni de service à distance.

SOLUTION :

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

DOCUMENTATION :

- Bulletin de sécurité Red Hat RHSA-2024:2950 du 22 mai 2024

<https://access.redhat.com/errata/RHSA-2024:2950>

- Bulletin de sécurité Red Hat RHSA-2024:3138 du 22 mai 2024

<https://access.redhat.com/errata/RHSA-2024:3138>

- Bulletin de sécurité Red Hat RHSA-2024:3306 du 23 mai 2024

<https://access.redhat.com/errata/RHSA-2024:3306>

- Bulletin de sécurité Red Hat RHSA-2024:3318 du 23 mai 2024

<https://access.redhat.com/errata/RHSA-2024:3318>

- Bulletin de sécurité Red Hat RHSA-2024:3319 du 23 mai 2024

<https://access.redhat.com/errata/RHSA-2024:3319>

- CVE-2019-13631

<https://www.cve.org/CVERecord?id=CVE-2019-13631>

- CVE-2019-15505

<https://www.cve.org/CVERecord?id=CVE-2019-15505>

- CVE-2020-25656

<https://www.cve.org/CVERecord?id=CVE-2020-25656>

- CVE-2021-3753

<https://www.cve.org/CVERecord?id=CVE-2021-3753>

- CVE-2021-4204

<https://www.cve.org/CVERecord?id=CVE-2021-4204>

- CVE-2022-0500

<https://www.cve.org/CVERecord?id=CVE-2022-0500>

- CVE-2022-23222

<https://www.cve.org/CVERecord?id=CVE-2022-23222>

- CVE-2022-3565

<https://www.cve.org/CVERecord?id=CVE-2022-3565>

- CVE-2022-40982

<https://www.cve.org/CVERecord?id=CVE-2022-40982>

- CVE-2022-45934

<https://www.cve.org/CVERecord?id=CVE-2022-45934>

- CVE-2023-1513

<https://www.cve.org/CVERecord?id=CVE-2023-1513>

- CVE-2023-24023

<https://www.cve.org/CVERecord?id=CVE-2023-24023>

- CVE-2023-25775

<https://www.cve.org/CVERecord?id=CVE-2023-25775>

- CVE-2023-28464

<https://www.cve.org/CVERecord?id=CVE-2023-28464>

- CVE-2023-31083

<https://www.cve.org/CVERecord?id=CVE-2023-31083>

- CVE-2023-3567

<https://www.cve.org/CVERecord?id=CVE-2023-3567>

- CVE-2023-37453

<https://www.cve.org/CVERecord?id=CVE-2023-37453>

- CVE-2023-38409

<https://www.cve.org/CVERecord?id=CVE-2023-38409>

- CVE-2023-39189

<https://www.cve.org/CVERecord?id=CVE-2023-39189>

- CVE-2023-39192

<https://www.cve.org/CVERecord?id=CVE-2023-39192>

- CVE-2023-39193

<https://www.cve.org/CVERecord?id=CVE-2023-39193>

- CVE-2023-39194

<https://www.cve.org/CVERecord?id=CVE-2023-39194>

- CVE-2023-39198

<https://www.cve.org/CVERecord?id=CVE-2023-39198>

- CVE-2023-4133

<https://www.cve.org/CVERecord?id=CVE-2023-4133>

- CVE-2023-4244

<https://www.cve.org/CVERecord?id=CVE-2023-4244>

- CVE-2023-42754

<https://www.cve.org/CVERecord?id=CVE-2023-42754>

- CVE-2023-42755

<https://www.cve.org/CVERecord?id=CVE-2023-42755>

- CVE-2023-45863

<https://www.cve.org/CVERecord?id=CVE-2023-45863>

- CVE-2023-51779

<https://www.cve.org/CVERecord?id=CVE-2023-51779>

- CVE-2023-51780

<https://www.cve.org/CVERecord?id=CVE-2023-51780>

- CVE-2023-52340

<https://www.cve.org/CVERecord?id=CVE-2023-52340>

- CVE-2023-52434

<https://www.cve.org/CVERecord?id=CVE-2023-52434>

- CVE-2023-52448

<https://www.cve.org/CVERecord?id=CVE-2023-52448>

- CVE-2023-52489

<https://www.cve.org/CVERecord?id=CVE-2023-52489>

- CVE-2023-52574

<https://www.cve.org/CVERecord?id=CVE-2023-52574>

- CVE-2023-52580

<https://www.cve.org/CVERecord?id=CVE-2023-52580>

- CVE-2023-52581

<https://www.cve.org/CVERecord?id=CVE-2023-52581>

- CVE-2023-52620

<https://www.cve.org/CVERecord?id=CVE-2023-52620>

- CVE-2023-6121

<https://www.cve.org/CVERecord?id=CVE-2023-6121>

- CVE-2023-6176

<https://www.cve.org/CVERecord?id=CVE-2023-6176>

- CVE-2023-6622

<https://www.cve.org/CVERecord?id=CVE-2023-6622>

- CVE-2023-6915

<https://www.cve.org/CVERecord?id=CVE-2023-6915>

- CVE-2023-6932

<https://www.cve.org/CVERecord?id=CVE-2023-6932>

- CVE-2024-0841

<https://www.cve.org/CVERecord?id=CVE-2024-0841>

- CVE-2024-1086

<https://www.cve.org/CVERecord?id=CVE-2024-1086>

- CVE-2024-25742

<https://www.cve.org/CVERecord?id=CVE-2024-25742>

- CVE-2024-25743

<https://www.cve.org/CVERecord?id=CVE-2024-25743>

- CVE-2024-26602

<https://www.cve.org/CVERecord?id=CVE-2024-26602>

- CVE-2024-26609

<https://www.cve.org/CVERecord?id=CVE-2024-26609>

- CVE-2024-26642

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

- CVE-2024-26643

<https://www.cve.org/CVERecord?id=CVE-2024-26643>

- CVE-2024-26671

<https://www.cve.org/CVERecord?id=CVE-2024-26671>

- CVE-2024-26673

<https://www.cve.org/CVERecord?id=CVE-2024-26673>

- CVE-2024-26804

<https://www.cve.org/CVERecord?id=CVE-2024-26804>