



DJ-CERT

Centre gouvernemental de  
veille, d'alerte et de réponse  
aux attaques informatiques

Agence Nationale  
des Systèmes d'information  
de l'état

Djibouti le, 26-07-2024

## **BULLETIN ALERTES**

Object	Multiplés vulnérabilités dans le noyau Linux de Red Hat
Référence	1194
Date de Publication	2024-07-26
Sévérité	Elevé

### **IMPACT :**

- Atteinte à la confidentialité des données
- Contournement de la politique de sécurité
- Déni de service
- Exécution de code arbitraire
- 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 - Telecommunications Update Service 8.4 x86\_64
- Red Hat Enterprise Linux for Real Time for NFV - Telecommunications Update Service 8.4 x86\_64
- 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 8.4 x86\_64
- Red Hat Enterprise Linux for x86\_64 - Update Services for SAP Solutions 9.2 x86\_64
- Red Hat Enterprise Linux Server - AUS 8.2 x86\_64
- Red Hat Enterprise Linux Server - AUS 8.4 x86\_64
- Red Hat Enterprise Linux Server - AUS 9.2 x86\_64
- Red Hat Enterprise Linux Server - TUS 8.4 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 8.4 ppc64le
- Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.2 ppc64le

## DÉSCRIPTION :

Plusieurs vulnérabilités ont été découvertes dans le noyau Linux de Red Hat. Certaines de ces vulnérabilités permettent à un attaquant d'exécuter du code arbitraire, d'élever ses privilèges ou de compromettre la confidentialité des données.

## SOLUTION :

Mettre à jour vos systèmes Linux de Red Hat. (se réfère à la documentation)

## DOCUMENTATION :

- Bulletin de sécurité Red Hat RHSA-2024:4577 du 16 juillet 2024

<https://access.redhat.com/errata/RHSA-2024:4577>

- Bulletin de sécurité Red Hat RHSA-2024:4729 du 23 juillet 2024

<https://access.redhat.com/errata/RHSA-2024:4729>

- Bulletin de sécurité Red Hat RHSA-2024:4731 du 23 juillet 2024

<https://access.redhat.com/errata/RHSA-2024:4731>

- Bulletin de sécurité Red Hat RHSA-2024:4823 du 24 juillet 2024

<https://access.redhat.com/errata/RHSA-2024:4823>

- Bulletin de sécurité Red Hat RHSA-2024:4831 du 24 juillet 2024

<https://access.redhat.com/errata/RHSA-2024:4831>

- CVE-2021-47459

<https://www.cve.org/CVERecord?id=CVE-2021-47459>

- CVE-2022-36402

<https://www.cve.org/CVERecord?id=CVE-2022-36402>

- CVE-2022-38457

<https://www.cve.org/CVERecord?id=CVE-2022-38457>

- CVE-2022-40133

<https://www.cve.org/CVERecord?id=CVE-2022-40133>

- CVE-2022-48743

<https://www.cve.org/CVERecord?id=CVE-2022-48743>

- CVE-2023-33951

<https://www.cve.org/CVERecord?id=CVE-2023-33951>

- CVE-2023-33952

<https://www.cve.org/CVERecord?id=CVE-2023-33952>

- CVE-2023-52434

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

- CVE-2023-52439

<https://www.cve.org/CVERecord?id=CVE-2023-52439>

- CVE-2023-52450

<https://www.cve.org/CVERecord?id=CVE-2023-52450>

- CVE-2023-52518

<https://www.cve.org/CVERecord?id=CVE-2023-52518>

- CVE-2023-52578

<https://www.cve.org/CVERecord?id=CVE-2023-52578>

- CVE-2023-52707

<https://www.cve.org/CVERecord?id=CVE-2023-52707>

- CVE-2023-52811

<https://www.cve.org/CVERecord?id=CVE-2023-52811>

- CVE-2023-5633

<https://www.cve.org/CVERecord?id=CVE-2023-5633>

- CVE-2023-6546

<https://www.cve.org/CVERecord?id=CVE-2023-6546>

- CVE-2024-1151

<https://www.cve.org/CVERecord?id=CVE-2024-1151>

- CVE-2024-21823

<https://www.cve.org/CVERecord?id=CVE-2024-21823>

- CVE-2024-26581



<https://www.cve.org/CVERecord?id=CVE-2024-26581>

- CVE-2024-26668

<https://www.cve.org/CVERecord?id=CVE-2024-26668>

- CVE-2024-26698

<https://www.cve.org/CVERecord?id=CVE-2024-26698>

- CVE-2024-26704

<https://www.cve.org/CVERecord?id=CVE-2024-26704>

- CVE-2024-26739

<https://www.cve.org/CVERecord?id=CVE-2024-26739>

- CVE-2024-26773

<https://www.cve.org/CVERecord?id=CVE-2024-26773>

- CVE-2024-26808

<https://www.cve.org/CVERecord?id=CVE-2024-26808>

- CVE-2024-26810

<https://www.cve.org/CVERecord?id=CVE-2024-26810>

- CVE-2024-26880

<https://www.cve.org/CVERecord?id=CVE-2024-26880>

- CVE-2024-26908

<https://www.cve.org/CVERecord?id=CVE-2024-26908>

- CVE-2024-26923

<https://www.cve.org/CVERecord?id=CVE-2024-26923>

- CVE-2024-26925

<https://www.cve.org/CVERecord?id=CVE-2024-26925>

- CVE-2024-26929

<https://www.cve.org/CVERecord?id=CVE-2024-26929>

- CVE-2024-26931

<https://www.cve.org/CVERecord?id=CVE-2024-26931>

- CVE-2024-26982

<https://www.cve.org/CVERecord?id=CVE-2024-26982>

- CVE-2024-27016

<https://www.cve.org/CVERecord?id=CVE-2024-27016>

- CVE-2024-27019

<https://www.cve.org/CVERecord?id=CVE-2024-27019>

- CVE-2024-27020

<https://www.cve.org/CVERecord?id=CVE-2024-27020>

- CVE-2024-27065

<https://www.cve.org/CVERecord?id=CVE-2024-27065>

- CVE-2024-27417

<https://www.cve.org/CVERecord?id=CVE-2024-27417>

- CVE-2024-35791

<https://www.cve.org/CVERecord?id=CVE-2024-35791>

- CVE-2024-35897

<https://www.cve.org/CVERecord?id=CVE-2024-35897>

- CVE-2024-35899

<https://www.cve.org/CVERecord?id=CVE-2024-35899>

- CVE-2024-35950

<https://www.cve.org/CVERecord?id=CVE-2024-35950>

- CVE-2024-36025

<https://www.cve.org/CVERecord?id=CVE-2024-36025>

- CVE-2024-36489

<https://www.cve.org/CVERecord?id=CVE-2024-36489>

- CVE-2024-36904

<https://www.cve.org/CVERecord?id=CVE-2024-36904>

- CVE-2024-36924

<https://www.cve.org/CVERecord?id=CVE-2024-36924>

- CVE-2024-36952

<https://www.cve.org/CVERecord?id=CVE-2024-36952>

- CVE-2024-36978

<https://www.cve.org/CVERecord?id=CVE-2024-36978>

- CVE-2024-38596

<https://www.cve.org/CVERecord?id=CVE-2024-38596>