DJ-CERT | Centre national de veille, d'alerte et de réponse aux attaques informatiques

Autorité Nationale de Cybersécurité

Djibouti le, 22-02-2025

BULLETIN ALERTES

Object	Multiples vulnérabilités dans le noyau Linux de Red Hat
Réference	1330
Date de Publication	2025-02-21
Sévérité	Elevé

IMPACT :

- Atteinte à la confidentialité des données
- Contournement de la politique de sécurité
- Déni de service

SYSTÉME AFFECTÉ :

- Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.4 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 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 9 x86_64
- Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.4 aarch64
- Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.4 aarch64
- Red Hat Enterprise Linux for ARM 64 9 aarch64
- Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.4 s390x
- Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.4 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 9 ppc64le
- Red Hat Enterprise Linux for Real Time 9 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 9 x86_64
- Red Hat Enterprise Linux Server - AUS 9.4 x86_64
- Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.4 ppc64le

DÉSCRIPTION :

Plusieurs vulnérabilités ont été identifiées dans le noyau Linux de Red Hat. Certaines d’entre elles peuvent être exploitées par un attaquant pour compromettre la confidentialité des données, contourner les politiques de sécurité ou provoquer un déni de service.

SOLUTION :

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

DOCUMENTATION :

- Bulletin de sécurité Red Hat RHSA-2025:1658 du 19 février 2025

https://access.redhat.com/errata/RHSA-2025:1658

- Bulletin de sécurité Red Hat RHSA-2025:1659 du 19 février 2025

https://access.redhat.com/errata/RHSA-2025:1659

- CVE-2023-52490

https://www.cve.org/CVERecord?id=CVE-2023-52490

- CVE-2023-52679

https://www.cve.org/CVERecord?id=CVE-2023-52679

- CVE-2024-23307

https://www.cve.org/CVERecord?id=CVE-2024-23307

- CVE-2024-26924

https://www.cve.org/CVERecord?id=CVE-2024-26924

- CVE-2024-26960

https://www.cve.org/CVERecord?id=CVE-2024-26960

- CVE-2024-27011

https://www.cve.org/CVERecord?id=CVE-2024-27011

- CVE-2024-27012

https://www.cve.org/CVERecord?id=CVE-2024-27012

- CVE-2024-27017

https://www.cve.org/CVERecord?id=CVE-2024-27017

- CVE-2024-35824

https://www.cve.org/CVERecord?id=CVE-2024-35824

- CVE-2024-35876

https://www.cve.org/CVERecord?id=CVE-2024-35876

- CVE-2024-36954

https://www.cve.org/CVERecord?id=CVE-2024-36954

- CVE-2024-46695

https://www.cve.org/CVERecord?id=CVE-2024-46695

- CVE-2024-50110

https://www.cve.org/CVERecord?id=CVE-2024-50110

- CVE-2024-50142

https://www.cve.org/CVERecord?id=CVE-2024-50142

- CVE-2024-50256

https://www.cve.org/CVERecord?id=CVE-2024-50256

- CVE-2024-50275

https://www.cve.org/CVERecord?id=CVE-2024-50275

- CVE-2024-53113

https://www.cve.org/CVERecord?id=CVE-2024-53113