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

Autorité Nationale de Cybersécurité

Djibouti le, 02-09-2025

BULLETIN ALERTES

Object	Multiples vulnérabilités dans le noyau Linux de Red Hat
Réference	1385
Date de Publication	2025-08-22
Sévérité	Elevé

IMPACT :

- Atteinte à la confidentialité des données
- Contournement de la politique de sécurité
- Déni de service
- Non spécifié par l'éditeur

SYSTÉME AFFECTÉ :

- Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 10.0 aarch64
- Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.4 aarch64
- Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.6 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 10.0 s390x
- Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.4 s390x
- Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.6 s390x
- Red Hat CodeReady Linux Builder for IBM z Systems 10 s390x

- Red Hat CodeReady Linux Builder for IBM z Systems 9 s390x
- Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 10.0 ppc64le
- Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.4 ppc64le
- Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.6 ppc64le
- Red Hat CodeReady Linux Builder for Power, little endian 10 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 10.0 x86_64
- Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.4 x86_64
- Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.6 x86_64
- Red Hat CodeReady Linux Builder for x86_64 10 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 - 4 years of updates 10.0 aarch64
- Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.0 aarch64
- Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.2 aarch64
- Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.4 aarch64
- Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.6 aarch64
- Red Hat Enterprise Linux for ARM 64 - Extended Update Support 10.0 aarch64
- Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.4 aarch64
- Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.6 aarch64
- Red Hat Enterprise Linux for ARM 64 10 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 - 4 years of updates 10.0 s390x
- Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.0 s390x
- Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.2 s390x
- Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.4 s390x
- Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.6 s390x
- Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 10.0 s390x
- Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.4 s390x
- Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.6 s390x
- Red Hat Enterprise Linux for IBM z Systems 10 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 - 4 years of support 10.0 ppc64le
- Red Hat Enterprise Linux for Power, little endian - Extended Update Support

10.0 ppc64le
- Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.4 ppc64le
- Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.6 ppc64le
- Red Hat Enterprise Linux for Power, little endian 10 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 for NFV 8 x86_64
- Red Hat Enterprise Linux for x86_64 - 4 years of updates 10.0 x86_64
- Red Hat Enterprise Linux for x86_64 - Extended Update Support 10.0 x86_64
- Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.4 x86_64
- Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.6 x86_64
- Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.0 x86_64
- Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.2 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 - Update Services for SAP Solutions 9.6 x86_64
- Red Hat Enterprise Linux for x86_64 10 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 8.2 x86_64
- Red Hat Enterprise Linux Server - AUS 9.2 x86_64
- Red Hat Enterprise Linux Server - AUS 9.4 x86_64
- Red Hat Enterprise Linux Server - AUS 9.6 x86_64
- Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.0 ppc64le
- Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.2 ppc64le
- Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.4 ppc64le
- Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.6 ppc64le

DÉSCRIPTION :

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

SOLUTION :

Consulter le bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

DOCUMENTATION :

- Bulletin de sécurité Red Hat RHSA-2025:13960 du 18 août 2025

https://access.redhat.com/errata/RHSA-2025:13960

- Bulletin de sécurité Red Hat RHSA-2025:13961 du 18 août 2025

https://access.redhat.com/errata/RHSA-2025:13961

- Bulletin de sécurité Red Hat RHSA-2025:13962 du 18 août 2025

https://access.redhat.com/errata/RHSA-2025:13962

- Bulletin de sécurité Red Hat RHSA-2025:14003 du 18 août 2025

https://access.redhat.com/errata/RHSA-2025:14003

- Bulletin de sécurité Red Hat RHSA-2025:14005 du 18 août 2025

https://access.redhat.com/errata/RHSA-2025:14005

- Bulletin de sécurité Red Hat RHSA-2025:14009 du 18 août 2025

https://access.redhat.com/errata/RHSA-2025:14009

- Bulletin de sécurité Red Hat RHSA-2025:14054 du 19 août 2025

https://access.redhat.com/errata/RHSA-2025:14054

- Bulletin de sécurité Red Hat RHSA-2025:14082 du 19 août 2025

https://access.redhat.com/errata/RHSA-2025:14082

- Bulletin de sécurité Red Hat RHSA-2025:14094 du 19 août 2025

https://access.redhat.com/errata/RHSA-2025:14094

- Bulletin de sécurité Red Hat RHSA-2025:14136 du 20 août 2025

https://access.redhat.com/errata/RHSA-2025:14136

- Référence CVE CVE-2021-47670

https://www.cve.org/CVERecord?id=CVE-2021-47670

- Référence CVE CVE-2022-49788

https://www.cve.org/CVERecord?id=CVE-2022-49788

- Référence CVE CVE-2022-50020

https://www.cve.org/CVERecord?id=CVE-2022-50020

- Référence CVE CVE-2022-50022

https://www.cve.org/CVERecord?id=CVE-2022-50022

- Référence CVE CVE-2022-50200

https://www.cve.org/CVERecord?id=CVE-2022-50200

- Référence CVE CVE-2023-53047

https://www.cve.org/CVERecord?id=CVE-2023-53047

- Référence CVE CVE-2024-28956

https://www.cve.org/CVERecord?id=CVE-2024-28956

- Référence CVE CVE-2024-57980

https://www.cve.org/CVERecord?id=CVE-2024-57980

- Référence CVE CVE-2025-21727

https://www.cve.org/CVERecord?id=CVE-2025-21727

- Référence CVE CVE-2025-21867

https://www.cve.org/CVERecord?id=CVE-2025-21867

- Référence CVE CVE-2025-21928

https://www.cve.org/CVERecord?id=CVE-2025-21928

- Référence CVE CVE-2025-21991

https://www.cve.org/CVERecord?id=CVE-2025-21991

- Référence CVE CVE-2025-22020

https://www.cve.org/CVERecord?id=CVE-2025-22020

- Référence CVE CVE-2025-22026

https://www.cve.org/CVERecord?id=CVE-2025-22026

- Référence CVE CVE-2025-22097

https://www.cve.org/CVERecord?id=CVE-2025-22097

- Référence CVE CVE-2025-37797

https://www.cve.org/CVERecord?id=CVE-2025-37797

- Référence CVE CVE-2025-37914

https://www.cve.org/CVERecord?id=CVE-2025-37914

- Référence CVE CVE-2025-38084

https://www.cve.org/CVERecord?id=CVE-2025-38084

- Référence CVE CVE-2025-38085

https://www.cve.org/CVERecord?id=CVE-2025-38085

- Référence CVE CVE-2025-38086

https://www.cve.org/CVERecord?id=CVE-2025-38086

- Référence CVE CVE-2025-38124

https://www.cve.org/CVERecord?id=CVE-2025-38124

- Référence CVE CVE-2025-38159

https://www.cve.org/CVERecord?id=CVE-2025-38159

- Référence CVE CVE-2025-38250

https://www.cve.org/CVERecord?id=CVE-2025-38250

- Référence CVE CVE-2025-38332

https://www.cve.org/CVERecord?id=CVE-2025-38332

- Référence CVE CVE-2025-38380

https://www.cve.org/CVERecord?id=CVE-2025-38380

- Référence CVE CVE-2025-38471

https://www.cve.org/CVERecord?id=CVE-2025-38471