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

Autorité Nationale de Cybersécurité

Djibouti le, 24-02-2026

BULLETIN ALERTES

Object	Multiples vulnérabilités dans le noyau Linux de Red Hat
Réference	1424
Date de Publication	2026-02-24
Sévérité	Elevé

IMPACT :

- Atteinte à l'intégrité des données
- Contournement de la politique de sécurité
- Déni de service à distance

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 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 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 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 Enterprise Linux for ARM 64 - 4 years of updates 10.0 aarch64
- 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 9.4 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 - 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 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 9.4 aarch64
- Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.6 aarch64
- Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.6 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 10.0 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 9.4 s390x
- Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.6 s390x
- Red Hat Enterprise Linux for IBM z Systems - 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 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 9.4 s390x
- Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.6 s390x
- Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.6 s390x
- Red Hat Enterprise Linux for Power, little endian - 4 years of support 10.0 ppc64le
- 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 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 9.4 ppc64le
- Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.6 ppc64le
- Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.6 ppc64le
- Red Hat Enterprise Linux for Real Time 8 x86_64
- 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 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 - 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 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 9.4 x86_64
- Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.6 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 9.4 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 - Update Services for SAP Solutions 9.6 x86_64
- Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.6 x86_64
- Red Hat Enterprise Linux Server - AUS 9.4 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 - AUS 9.6 x86_64
- 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 9.4 ppc64le
- Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.6 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. Elles peuvent être exploitées par un attaquant pour provoquer un déni de service à distance, altérer l’intégrité des données ou contourner les mécanismes de sécurité.

SOLUTION :

Consulter le bulletin de sécurité de l'éditeur afin d'obtenir les correctifs (cf. section Documentation).

DOCUMENTATION :

- Bulletin de sécurité Red Hat RHSA-2026:2759 du 16 février 2026

https://access.redhat.com/errata/RHSA-2026:2759

- Bulletin de sécurité Red Hat RHSA-2026:2761 du 16 février 2026

https://access.redhat.com/errata/RHSA-2026:2761

- Bulletin de sécurité Red Hat RHSA-2026:2766 du 17 février 2026

https://access.redhat.com/errata/RHSA-2026:2766

- Bulletin de sécurité Red Hat RHSA-2026:2821 du 17 février 2026

https://access.redhat.com/errata/RHSA-2026:2821

- Référence CVE CVE-2023-53762

https://www.cve.org/CVERecord?id=CVE-2023-53762

- Référence CVE CVE-2025-37882

https://www.cve.org/CVERecord?id=CVE-2025-37882

- Référence CVE CVE-2025-38051

https://www.cve.org/CVERecord?id=CVE-2025-38051

- Référence CVE CVE-2025-38349

https://www.cve.org/CVERecord?id=CVE-2025-38349

- Référence CVE CVE-2025-38383

https://www.cve.org/CVERecord?id=CVE-2025-38383

- Référence CVE CVE-2025-38415

https://www.cve.org/CVERecord?id=CVE-2025-38415

- Référence CVE CVE-2025-38730

https://www.cve.org/CVERecord?id=CVE-2025-38730

- Référence CVE CVE-2025-39760

https://www.cve.org/CVERecord?id=CVE-2025-39760

- Référence CVE CVE-2025-39933

https://www.cve.org/CVERecord?id=CVE-2025-39933

- Référence CVE CVE-2025-40168

https://www.cve.org/CVERecord?id=CVE-2025-40168

- Référence CVE CVE-2025-40269

https://www.cve.org/CVERecord?id=CVE-2025-40269

- Référence CVE CVE-2025-40271

https://www.cve.org/CVERecord?id=CVE-2025-40271

- Référence CVE CVE-2025-40294

https://www.cve.org/CVERecord?id=CVE-2025-40294

- Référence CVE CVE-2025-40304

https://www.cve.org/CVERecord?id=CVE-2025-40304

- Référence CVE CVE-2025-68349

https://www.cve.org/CVERecord?id=CVE-2025-68349