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

Autorité Nationale de Cybersécurité

Djibouti le, 09-09-2024

BULLETIN ALERTES

Object	Multiples vulnérabilités dans le noyau Linux de Red Hat
Réference	1241
Date de Publication	2024-09-09
Sévérité	Elevé

IMPACT :

- Déni de service

SYSTÉME 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 - 4 years of updates 9.2 aarch64
- Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.2 aarch64
- Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.2 s390x
- 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 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 8.4 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 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 :

De multiples vulnérabilités ont été découvertes dans le noyau Linux de Red Hat. Elles permettent à un attaquant de provoquer un déni de service.

SOLUTION :

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

DOCUMENTATION :

- Bulletin de sécurité Red Hat RHSA-2024:6156 du 03 septembre 2024

https://access.redhat.com/errata/RHSA-2024:6156

- Bulletin de sécurité Red Hat RHSA-2024:6267 du 04 septembre 2024

https://access.redhat.com/errata/RHSA-2024:6267

- Bulletin de sécurité Red Hat RHSA-2024:6268 du 04 septembre 2024

https://access.redhat.com/errata/RHSA-2024:6268

- CVE-2022-48799

https://www.cve.org/CVERecord?id=CVE-2022-48799

- CVE-2024-26946

https://www.cve.org/CVERecord?id=CVE-2024-26946

- CVE-2024-35839

https://www.cve.org/CVERecord?id=CVE-2024-35839

- CVE-2024-35875

https://www.cve.org/CVERecord?id=CVE-2024-35875

- CVE-2024-35895

https://www.cve.org/CVERecord?id=CVE-2024-35895

- CVE-2024-38540

https://www.cve.org/CVERecord?id=CVE-2024-38540

- CVE-2024-38570

https://www.cve.org/CVERecord?id=CVE-2024-38570

- CVE-2024-39502

https://www.cve.org/CVERecord?id=CVE-2024-39502

- CVE-2024-40914

https://www.cve.org/CVERecord?id=CVE-2024-40914

- CVE-2024-40956

https://www.cve.org/CVERecord?id=CVE-2024-40956

- CVE-2024-40978

https://www.cve.org/CVERecord?id=CVE-2024-40978

- CVE-2024-40983

https://www.cve.org/CVERecord?id=CVE-2024-40983

- CVE-2024-40995

https://www.cve.org/CVERecord?id=CVE-2024-40995

- CVE-2024-41044

https://www.cve.org/CVERecord?id=CVE-2024-41044

- CVE-2024-41090

https://www.cve.org/CVERecord?id=CVE-2024-41090

- CVE-2024-41091

https://www.cve.org/CVERecord?id=CVE-2024-41091

- CVE-2024-42102

https://www.cve.org/CVERecord?id=CVE-2024-42102

- CVE-2024-42131

https://www.cve.org/CVERecord?id=CVE-2024-42131