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

Autorité Nationale de Cybersécurité

Djibouti le, 02-06-2024

BULLETIN ALERTES

Object	Multiples Vulnérabilités dans le noyau Linux de RedHat
Réference	1156
Date de Publication	2024-05-31
Sévérité	Elevé

IMPACT :

- Atteinte à la confidentialité des données
- Déni de service
- Non spécifié par l'éditeur
- Élévation de privilèges

SYSTÉME AFFECTÉ :

- Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 8.6 aarch64
- Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.0 aarch64
- 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 9.0 s390x
- 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 8.6 ppc64le
- Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.0 ppc64le
- 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 8.6 x86_64
- Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.0 x86_64
- 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 8.6 aarch64
- Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.0 aarch64
- Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.2 aarch64
- Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 8.6 s390x
- Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.0 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 8.6 ppc64le
- Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.0 ppc64le
- 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 9.0 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 9.0 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 8.6 x86_64
- Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.0 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 8.6 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 Server - AUS 8.6 x86_64
- Red Hat Enterprise Linux Server - AUS 9.2 x86_64
- Red Hat Enterprise Linux Server - TUS 8.6 x86_64
- Red Hat Enterprise Linux Server for ARM 64 - 4 years of updates 9.0 aarch64
- 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 9.0 s390x
- 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 8.6 ppc64le
- 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 Virtualization Host 4 for RHEL 8 x86_64

DÉSCRIPTION :

Des nombreuses vulnérabilités ont été découvertes dans le noyau Linux de RedHat susmentionné.

Elles permettent à un attaquant de provoquer une élévation de privilèges, une atteinte à la confidentialité des données, un déni de service.

SOLUTION :

Mettre à jour vos systèmes RedHat.(se réfère à la documentation)

DOCUMENTATION :

- Bulletin de sécurité Red Hat RHSA-2024:3414 du 28 mai 2024

https://access.redhat.com/errata/RHSA-2024:3414

- Bulletin de sécurité Red Hat RHSA-2024:3421 du 28 mai 2024

https://access.redhat.com/errata/RHSA-2024:3421

- Bulletin de sécurité Red Hat RHSA-2024:3460 du 29 mai 2024

https://access.redhat.com/errata/RHSA-2024:3460

- Bulletin de sécurité Red Hat RHSA-2024:3461 du 29 mai 2024

https://access.redhat.com/errata/RHSA-2024:3461

- Bulletin de sécurité Red Hat RHSA-2024:3462 du 29 mai 2024

https://access.redhat.com/errata/RHSA-2024:3462

- CVE-2021-47013

https://www.cve.org/CVERecord?id=CVE-2021-47013

- CVE-2023-3006

https://www.cve.org/CVERecord?id=CVE-2023-3006

- CVE-2023-4244

https://www.cve.org/CVERecord?id=CVE-2023-4244

- CVE-2023-52578

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

- CVE-2023-52628

https://www.cve.org/CVERecord?id=CVE-2023-52628

- CVE-2023-6240

https://www.cve.org/CVERecord?id=CVE-2023-6240

- CVE-2023-6817

https://www.cve.org/CVERecord?id=CVE-2023-6817

- CVE-2024-1086

https://www.cve.org/CVERecord?id=CVE-2024-1086

- CVE-2024-25742

https://www.cve.org/CVERecord?id=CVE-2024-25742

- CVE-2024-25743

https://www.cve.org/CVERecord?id=CVE-2024-25743

- CVE-2024-26586

https://www.cve.org/CVERecord?id=CVE-2024-26586

- CVE-2024-26642

https://www.cve.org/CVERecord?id=CVE-2024-26642

- CVE-2024-26643

https://www.cve.org/CVERecord?id=CVE-2024-26643

- CVE-2024-26673

https://www.cve.org/CVERecord?id=CVE-2024-26673

- CVE-2024-26735

https://www.cve.org/CVERecord?id=CVE-2024-26735

- CVE-2024-26804

https://www.cve.org/CVERecord?id=CVE-2024-26804

- CVE-2024-26828

https://www.cve.org/CVERecord?id=CVE-2024-26828

- CVE-2024-26993

https://www.cve.org/CVERecord?id=CVE-2024-26993