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

Autorité Nationale de Cybersécurité

Djibouti le, 17-03-2024

BULLETIN ALERTES

Object	Multiples vulnérabilités dans le noyau Linux de RedHat
Réference	1129
Date de Publication	2024-03-17
Sévérité	Critique

IMPACT :

- Atteinte à l'intégrité des données
- Atteinte à la confidentialité des données
- Contournement de la politique de sécurité
- Déni de service à distance
- Exécution de code arbitraire à distance
- Élévation de privilèges

SYSTÉME AFFECTÉ :

- Red Hat CodeReady Linux Builder pour ARM 64 - Extended Update Support9.0aarch64
- Red Hat CodeReady Linux Builder pour ARM 64 - Extended Update Support9.2aarch64
- Red Hat CodeReady Linux Builder pour IBM z Systems - Extended Update Support 9.0 s390x
- Red Hat CodeReady Linux Builder pour IBM z Systems - Extended Update Support 9.2 s390x
- Red Hat CodeReady Linux Builder pour Power, little endian- Extended Update Support 9.0 ppc64le
- Red Hat CodeReady Linux Builder pour Power, little endian- Extended Update Support 9.2 ppc64le
- Red Hat CodeReady Linux Builder pour x86_64 - Extended Update Support9.0x86_64
- Red Hat CodeReady Linux Builder pour x86_64 - Extended Update Support9.2x86_64
- Red Hat Enterprise Linux Desktop 7 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 - Extended Life Cycle Support (for IBMzSystems) 7 s390x
- Red Hat Enterprise Linux Server - Extended Life Cycle Support 7x86_64
- Red Hat Enterprise Linux Server - TUS 8.2 x86_64
- Red Hat Enterprise Linux Server 7 x86_64
- Red Hat Enterprise Linux Server pour ARM 64 - 4 years of updates 9.0aarch64
- Red Hat Enterprise Linux Server pour ARM 64 - 4 years of updates 9.2aarch64
- Red Hat Enterprise Linux Server pour IBM z Systems - 4 yearsof updates 9.0s390x
- Red Hat Enterprise Linux Server pour IBM z Systems - 4 yearsof updates 9.2s390x
- Red Hat Enterprise Linux Server pour Power LE - Update Services pour SAP Solutions 8.2 ppc64le
- Red Hat Enterprise Linux Server pour Power LE - Update Services pour SAP Solutions 9.0 ppc64le
- Red Hat Enterprise Linux Server pour Power LE - Update Services pour SAP Solutions 9.2 ppc64le
- Red Hat Enterprise Linux Workstation 7 x86_64
- Red Hat Enterprise Linux pour ARM 64 - Extended Update Support 9.0aarch64
- Red Hat Enterprise Linux pour ARM 64 - Extended Update Support 9.2aarch64
- Red Hat Enterprise Linux pour IBM z Systems - Extended Update Support9.0s390x
- Red Hat Enterprise Linux pour IBM z Systems - Extended Update Support 9.2s390x

- Red Hat Enterprise Linux pour IBM z Systems 7 s390x
- Red Hat Enterprise Linux pour Power, big endian 7 ppc64
- Red Hat Enterprise Linux pour Power, little endian – Extended Update Support 9.0 ppc64le
- Red Hat Enterprise Linux pour Power, little endian – Extended Update Support 9.2 ppc64le
- Red Hat Enterprise Linux pour Power, little endian 7 ppc64le
- Red Hat Enterprise Linux pour Real Time – Telecommunications Update Service 8.2 x86_64
- Red Hat Enterprise Linux pour Real Time 7 x86_64
- Red Hat Enterprise Linux pour Real Time pour NFV – Telecommunications Update Service 8.2 x86_64
- Red Hat Enterprise Linux pour Real Time pour NFV 7 x86_64
- Red Hat Enterprise Linux pour Real Time pour NFV pour x86_64- 4 years of updates 9.0 x86_64
- Red Hat Enterprise Linux pour Real Time pour NFV pour x86_64- 4 years of updates 9.2 x86_64
- Red Hat Enterprise Linux pour Real Time pour x86_64 - 4 years of updates9.0x86_64
- Red Hat Enterprise Linux pour Real Time pour x86_64 - 4 years of updates 9.2x86_64
- Red Hat Enterprise Linux pour Scientific Computing 7 x86_64
- Red Hat Enterprise Linux pour x86_64 - Extended Update Support 9.0x86_64
- Red Hat Enterprise Linux pour x86_64 - Extended Update Support 9.2x86_64
- Red Hat Enterprise Linux pour x86_64 - Update Services pour SAP Solutions 8.2 x86_64
- Red Hat Enterprise Linux pour x86_64 - Update Services pour SAP Solutions 9.0 x86_64
- Red Hat Enterprise Linux pour x86_64 - Update Services pour SAP Solutions 9.2 x86_64

DÉSCRIPTION :

De multiples vulnérabilités ont été découvertes dans le noyau Linux de RedHat. Certaines d'entre elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance, un déni de service à distance et une élévation de privilèges.

SOLUTION :

Mettre à jour linux redhat

DOCUMENTATION :

CVE-2024-26602

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-26602

CVE-2024-1086

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-1086

CVE-2024-0646

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-0646

CVE-2023-7192

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-7192

CVE-2023-6932

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-693

CVE-2023-6817

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-6817

CVE-2023-6546

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-6546

CVE-2023-5717

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-5717

CVE-2023-5178

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-5178

CVE-2023-4921

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-4921

CVE-2023-4623

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-4623

CVE-2023-4622

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-4622

CVE-2023-45871

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-45871

CVE-2023-4459

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-4459

CVE-2023-40283

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-40283

CVE-2023-38409

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-38409

CVE-2023-3611

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-3611

CVE-2023-3609

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-3609

CVE-2023-35001

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-35001

CVE-2023-3390

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-3390

CVE-2023-3268

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-3268

CVE-2023-31436

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-31436

CVE-2023-2176

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-2176

CVE-2023-2166

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-2166

CVE-2023-2163

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-2163

CVE-2023-1192

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-1192

CVE-2022-42896

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-42896

CVE-2022-41858

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41858

CVE-2022-40982

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-40982

CVE-2022-38096

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-38096

CVE-2022-3545

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-3545

CVE-2022-0480

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0480