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

Autorité Nationale de Cybersécurité

Djibouti le, 11-02-2024

BULLETIN ALERTES

Object	Multiples vulnérabilités dans le noyau Linux de RedHat
Réference	1106
Date de Publication	2024-02-11
Sévérité	Critique

IMPACT :

- Non spécifié par l'éditeur
- Exécution de code arbitraire
- Déni de service à distance
- Contournement de la politique de sécurité
- Atteinte à l'intégrité des données
- Atteinte à la confidentialité des données
- 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 Power, little endian - Extended Update Support 8.6 ppc64le
- Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 8.6 x86_64
- Red Hat Enterprise Linux Server - AUS 8.6 x86_64
- Red Hat Enterprise Linux Server - TUS 8.6 x86_64
- Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.6 ppc64le
- Red Hat Enterprise Linux for ARM 64 - Extended Update Support 8.6 aarch64
- Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 8.6 s390x
- Red Hat Enterprise Linux for Power, little endian - Extended Update Support 8.6 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 8.6 x86_64
- Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.6 x86_64
- Red Hat Virtualization Host 4

DÉSCRIPTION :

De multiples vulnérabilités ont été découvertes dans le noyau Linux deRedHat.Certaines d'entre elles permettent à un attaquant de provoquer un problèmedesécurité non spécifié par l'éditeur, une exécution de code arbitraire et undéni deservice à distance.

SOLUTION :

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

DOCUMENTATION :

- Bulletin de sécurité Redhat :

https://access.redhat.com/errata/RHSA-2024:0724

- CVE-2021-30002
  https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30002
- CVE-2021-34866
  https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34866
- CVE-2021-3640
  https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-3640
- CVE-2021-4204
  https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-4204
- CVE-2022-01684
  https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-01684
- CVE-2022-0500
  https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0500
- CVE-2022-0617
  https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0617
- CVE-2022-1462
  https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1462
- CVE-2022-2078
  https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-2078
- CVE-2022-21499
  https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21499
- CVE-2022-24448
  https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-24448
- CVE-2022-25265
  https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-25265
- CVE-2022-2586
  https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-2586
- CVE-2022-2663
  https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-2663
- CVE-2022-28388
  https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-28388
- CVE-2022-28390
  https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-28390
- CVE-2022-28893
  https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-28893