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

Autorité Nationale de Cybersécurité

Djibouti le, 03-03-2024

BULLETIN ALERTES

Object	Multiples Vulnérabilités dans le noyau Linux de RedHat
Réference	1122
Date de Publication	2024-03-03
Sévérité	Elevé

IMPACT :

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

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 Server - AUS 7.6 x86_64
- Red Hat Enterprise Linux Server - AUS 7.7 x86_64
- Red Hat Enterprise Linux Server - AUS 9.2 x86_64
- 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 9.2 s390x
- Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.2 ppc64le
- Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.2 aarch64
- 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 9.2 x86_64

DÉSCRIPTION :

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

Ces vulnérabilités permettent à un attaquant de provoquer une atteinte à la confidentialité des données, une élévation de privilèges et une exécution de code arbitraire à distance.

SOLUTION :

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

DOCUMENTATION :

- Bulletin de sécurité RedHat 26-02-2024
  https://access.redhat.com/errata/RHSA-2024:0980
- Bulletin de sécurité RedHat 27-02-2024
  https://access.redhat.com/errata/RHSA-2024:0999
- Bulletin de sécurité RedHat 28-02-2024
  https://access.redhat.com/errata/RHSA-2024:1018
- CVE-2022-38096
  https://www.cve.org/CVERecord?id=CVE-2022-38096
- CVE-2022-42896
  https://www.cve.org/CVERecord?id=CVE-2022-42896
- CVE-2023-3609
  https://www.cve.org/CVERecord?id=CVE-2023-3609
- CVE-2023-4244
  https://www.cve.org/CVERecord?id=CVE-2023-4244
- CVE-2023-42753
  https://www.cve.org/CVERecord?id=CVE-2023-42753
- CVE-2023-45871
  https://www.cve.org/CVERecord?id=CVE-2023-45871
- CVE-2023-4921
  https://www.cve.org/CVERecord?id=CVE-2023-4921
- CVE-2023-51042
  https://www.cve.org/CVERecord?id=CVE-2023-51042
- CVE-2023-51043
  https://www.cve.org/CVERecord?id=CVE-2023-51043
- CVE-2023-6546
  https://www.cve.org/CVERecord?id=CVE-2023-6546
- CVE-2023-6817
  https://www.cve.org/CVERecord?id=CVE-2023-6817
- CVE-2023-6931
  https://www.cve.org/CVERecord?id=CVE-2023-6931
- CVE-2024-0193
  https://www.cve.org/CVERecord?id=CVE-2024-0193
- CVE-2024-1085
  https://www.cve.org/CVERecord?id=CVE-2024-1085
- CVE-2024-1086
  https://www.cve.org/CVERecord?id=CVE-2024-1086