BULLETIN DE CYBERSECURITE

TLP: CLEAR = Diffusion sans restriction.

Les documents avec ce marquage peuvent être diffusés sans restriction, sous réserve du respect des règles de copyright. Les bénéficiaires peuvent partager les documents et informations sans restriction.

Multiples vulnérabilités dans le noyau Linux de RedHat			
Source(s)	Bulletins de sécurité RedHat du 02 et 03 avril 2024		
CVE	CVE-2023-6546 ; CVE-2024-0565		
Auditoire	Tous publics		
Référence	CICERT-BS-2024-043	**Date de 1ère publication**	08/04/2024
Version	1.0	**Dernière mise à jour**	08/04/2024
CVSS	7.4	**Criticité**	Élevé

RISQUES :

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

SYSTEMES AFFECTES :

- Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 8.6 aarch64
- Red Hat CodeReady Linux Builder for ARM 64 8 aarch64
- Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 8.6 ppc64le
- Red Hat CodeReady Linux Builder for Power, little endian 8 ppc64le
- Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 8.6 x86_64
- Red Hat CodeReady Linux Builder for x86_64 8 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 ARM 64 8 aarch64
- Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 8.6 s390x
- Red Hat Enterprise Linux for IBM z Systems 8 s390x
- Red Hat Enterprise Linux for Power, little endian - Extended Update Support 8.6 ppc64le
- Red Hat Enterprise Linux for Power, little endian 8 ppc64le
- Red Hat Enterprise Linux for Real Time 8 x86_64
- Red Hat Enterprise Linux for Real Time for NFV 8 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 Enterprise Linux for x86_64 8 x86_64
- Red Hat Virtualization Host 4 for RHEL 8 x86_64

RESUME

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, un déni de service à distance et une élévation de privilèges.

RECOMMANDATIONS

Appliquer les recommandations de l'éditeur (Bulletin de sécurité REDHAT)

REFERENCES

- Bulletin de sécurité RedHat RHSA-2024:1607 du 02 avril 2024
  https://access.redhat.com/errata/RHSA-2024:1607
- Bulletin de sécurité RedHat RHSA-2024:1653 du 03 avril 2024
  https://access.redhat.com/errata/RHSA-2024:1653
- Bulletin de sécurité RedHat RHSA-2024:1614 du 02 avril 2024
  https://access.redhat.com/errata/RHSA-2024:1614
- Référence CVE CVE-2021-33631
  https://www.cve.org/CVERecord?id=CVE-2021-33631
- Référence CVE CVE-2022-38096
  https://www.cve.org/CVERecord?id=CVE-2022-38096
- Référence CVE CVE-2023-1118
  https://www.cve.org/CVERecord?id=CVE-2023-1118
- Référence CVE CVE-2023-51042
  https://www.cve.org/CVERecord?id=CVE-2023-51042
- Référence CVE CVE-2023-6546
  https://www.cve.org/CVERecord?id=CVE-2023-6546
- Référence CVE CVE-2023-6931
  https://www.cve.org/CVERecord?id=CVE-2023-6931
- Référence CVE CVE-2024-0565
  https://www.cve.org/CVERecord?id=CVE-2024-0565
- Référence CVE CVE-2024-1086
  https://www.cve.org/CVERecord?id=CVE-2024-1086
- Référence CVE CVE-2024-26602
  https://www.cve.org/CVERecord?id=CVE-2024-26602