Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

S . G . D . S . N
Agence nationale
de la sécurité des
systèmes d'information

Paris, le 01 décembre 2023
N° CERTFR-2023-AVI-0989

Affaire suivie par: CERT-FR

AVIS DU CERT-FR

Objet: Multiples vulnérabilités dans le noyau Linux de RedHat

Gestion du document

Référence	CERTFR-2023-AVI-0989
Titre	Multiples vulnérabilités dans le noyau Linux de RedHat
Date de la première version	01 décembre 2023
Date de la dernière version	01 décembre 2023
Source(s)	Bulletin de sécurité RedHat RHSA-2023:7539 du 28 novembre 2023 Bulletin de sécurité RedHat RHSA-2023:7548 du 28 novembre 2023 Bulletin de sécurité RedHat RHSA-2023:7549 du 28 novembre 2023 Bulletin de sécurité RedHat RHSA-2023:7551 du 28 novembre 2023 Bulletin de sécurité RedHat RHSA-2023:7557 du 28 novembre 2023
Pièce(s) jointe(s)	Aucune(s)

Tableau 1: Gestion du document

Une gestion de version détaillée se trouve à la fin de ce document.

Risque(s)

- Atteinte à la confidentialité des données
- Exécution de code arbitraire à distance

- Déni de service à distance
- Elévation de privilèges

Systèmes affectés

- Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 8.8 aarch64
- Red Hat CodeReady Linux Builder for ARM 64 8 aarch64
- Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 8.8 ppc64le
- Red Hat CodeReady Linux Builder for Power, little endian 8 ppc64le
- Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 8.8 x86_64
- Red Hat CodeReady Linux Builder for x86_64 8 x86_64
- Red Hat Enterprise Linux Server - AUS 8.4 x86_64
- Red Hat Enterprise Linux Server - TUS 8.4 x86_64
- Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.4 ppc64le
- Red Hat Enterprise Linux for ARM 64 - Extended Update Support 8.8 aarch64
- Red Hat Enterprise Linux for ARM 64 8 aarch64
- Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 8.8 s390x
- Red Hat Enterprise Linux for IBM z Systems 8 s390x
- Red Hat Enterprise Linux for Power, little endian - Extended Update Support 8.8 ppc64le
- Red Hat Enterprise Linux for Power, little endian 8 ppc64le
- Red Hat Enterprise Linux for Real Time - Telecommunications Update Service 8.4 x86_64
- Red Hat Enterprise Linux for Real Time 8 x86_64
- Red Hat Enterprise Linux for Real Time for NFV - Telecommunications Update Service 8.4 x86_64
- Red Hat Enterprise Linux for Real Time for NFV 8 x86_64
- Red Hat Enterprise Linux for x86_64 - Extended Update Support 8.8 x86_64
- Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.4 x86_64
- Red Hat Enterprise Linux for x86_64 8 x86_64

Résumé

De multiples vulnérabilités ont été découvertes dans le noyau Linux de RedHat. Elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance, une atteinte à la confidentialité des données et un déni de service à distance.

Solution

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

Documentation

- Bulletin de sécurité RedHat RHSA-2023:7551 du 28 novembre 2023
  https://access.redhat.com/errata/RHSA-2023:7551
- Bulletin de sécurité RedHat RHSA-2023:7549 du 28 novembre 2023
  https://access.redhat.com/errata/RHSA-2023:7549
- Bulletin de sécurité RedHat RHSA-2023:7548 du 28 novembre 2023
  https://access.redhat.com/errata/RHSA-2023:7548
- Bulletin de sécurité RedHat RHSA-2023:7539 du 28 novembre 2023
  https://access.redhat.com/errata/RHSA-2023:7539

- Bulletin de sécurité RedHat RHSA-2023:7557 du 28 novembre 2023
https://access.redhat.com/errata/RHSA-2023:7557
- Référence CVE CVE-2022-40982
https://www.cve.org/CVERecord?id=CVE-2022-40982
- Référence CVE CVE-2022-45884
https://www.cve.org/CVERecord?id=CVE-2022-45884
- Référence CVE CVE-2022-45886
https://www.cve.org/CVERecord?id=CVE-2022-45886
- Référence CVE CVE-2022-45919
https://www.cve.org/CVERecord?id=CVE-2022-45919
- Référence CVE CVE-2023-1192
https://www.cve.org/CVERecord?id=CVE-2023-1192
- Référence CVE CVE-2023-20593
https://www.cve.org/CVERecord?id=CVE-2023-20593
- Référence CVE CVE-2023-2163
https://www.cve.org/CVERecord?id=CVE-2023-2163
- Référence CVE CVE-2023-3609
https://www.cve.org/CVERecord?id=CVE-2023-3609
- Référence CVE CVE-2023-3812
https://www.cve.org/CVERecord?id=CVE-2023-3812
- Référence CVE CVE-2023-38409
https://www.cve.org/CVERecord?id=CVE-2023-38409
- Référence CVE CVE-2023-4128
https://www.cve.org/CVERecord?id=CVE-2023-4128
- Référence CVE CVE-2023-4206
https://www.cve.org/CVERecord?id=CVE-2023-4206
- Référence CVE CVE-2023-4207
https://www.cve.org/CVERecord?id=CVE-2023-4207
- Référence CVE CVE-2023-4208
https://www.cve.org/CVERecord?id=CVE-2023-4208
- Référence CVE CVE-2023-42753
https://www.cve.org/CVERecord?id=CVE-2023-42753
- Référence CVE CVE-2023-4732
https://www.cve.org/CVERecord?id=CVE-2023-4732
- Référence CVE CVE-2023-5178
https://www.cve.org/CVERecord?id=CVE-2023-5178

Gestion détaillée du document

le 01 décembre 2023

Version initiale