



.....
Centre de Veille de Détection et de
Réaction aux Attaques Informatiques

BULLETIN DE SECURITE

Titre	Vulnérabilités affectant le noyau de Redhat
Numéro de Référence	58501411/25
Date de publication	14 novembre 2025
Risque	Important
Impact	Important

Systèmes affectés

- Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.4 aarch64
- Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.6 aarch64
- Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 10.0 aarch64
- Red Hat CodeReady Linux Builder for ARM 64 8 aarch64
- Red Hat CodeReady Linux Builder for ARM 64 9 aarch64
- Red Hat CodeReady Linux Builder for ARM 64 10 aarch64
- Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.4 s390x
- Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.6 s390x
- Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 10.0 s390x
- Red Hat CodeReady Linux Builder for IBM z Systems 9 s390x
- Red Hat CodeReady Linux Builder for IBM z Systems 10 s390x
- Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.4 ppc64le
- Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.6 ppc64le
- Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 10.0 ppc64le
- Red Hat CodeReady Linux Builder for Power, little endian 8 ppc64le
- Red Hat CodeReady Linux Builder for Power, little endian 9 ppc64le
- Red Hat CodeReady Linux Builder for Power, little endian 10 ppc64le
- Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.4 x86_64
- Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.6 x86_64
- Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 10.0 x86_64

- Red Hat CodeReady Linux Builder for x86_64 8 x86_64
- Red Hat CodeReady Linux Builder for x86_64 9 x86_64
- Red Hat CodeReady Linux Builder for x86_64 10 x86_64
- Red Hat Enterprise Linux Server - AUS 8.6 x86_64
- Red Hat Enterprise Linux Server - AUS 9.2 x86_64
- Red Hat Enterprise Linux Server - AUS 9.4 x86_64
- Red Hat Enterprise Linux Server - AUS 9.6 x86_64
- Red Hat Enterprise Linux Server - TUS 8.6 x86_64
- Red Hat Enterprise Linux Server - TUS 8.8 x86_64
- Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.6 ppc64le
- Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.8 ppc64le
- Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.0 ppc64le
- Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.2 ppc64le
- Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.4 ppc64le
- Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.6 ppc64le
- Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.0 aarch64
- Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.2 aarch64
- Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.4 aarch64
- Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.6 aarch64
- Red Hat Enterprise Linux for ARM 64 - 4 years of updates 10.0 aarch64
- Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.4 aarch64
- Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.6 aarch64
- Red Hat Enterprise Linux for ARM 64 - Extended Update Support 10.0 aarch64
- Red Hat Enterprise Linux for ARM 64 8 aarch64
- Red Hat Enterprise Linux for ARM 64 9 aarch64
- Red Hat Enterprise Linux for ARM 64 10 aarch64
- Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.0 s390x
- Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.2 s390x
- Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.4 s390x
- Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.6 s390x
- Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 10.0 s390x
- Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.4 s390x
- Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.6 s390x
- Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 10.0 s390x
- Red Hat Enterprise Linux for IBM z Systems 8 s390x
- Red Hat Enterprise Linux for IBM z Systems 9 s390x
- Red Hat Enterprise Linux for IBM z Systems 10 s390x
- Red Hat Enterprise Linux for Power, little endian - 4 years of support 10.0 ppc64le
- Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.4 ppc64le

- Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.6 ppc64le
- Red Hat Enterprise Linux for Power, little endian - Extended Update Support 10.0 ppc64le
- Red Hat Enterprise Linux for Power, little endian 8 ppc64le
- Red Hat Enterprise Linux for Power, little endian 9 ppc64le
- Red Hat Enterprise Linux for Power, little endian 10 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 Real Time for x86_64 - Extended Life Cycle Support 7 x86_64
- Red Hat Enterprise Linux for x86_64 - 4 years of updates 10.0 x86_64
- Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.4 x86_64
- Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.6 x86_64
- Red Hat Enterprise Linux for x86_64 - Extended Update Support 10.0 x86_64
- Red Hat Enterprise Linux for x86_64 - Extended Update Support Extension 8.6 x86_64
- Red Hat Enterprise Linux for x86_64 - Extended Update Support Extension 8.8 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 - Update Services for SAP Solutions 8.8 x86_64
- Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.0 x86_64
- Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.2 x86_64
- Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.4 x86_64
- Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.6 x86_64
- Red Hat Enterprise Linux for x86_64 8 x86_64
- Red Hat Enterprise Linux for x86_64 9 x86_64
- Red Hat Enterprise Linux for x86_64 10 x86_64

Identificateurs externes

- | | | | |
|------------------|----------------|----------------|----------------|
| • CVE-2022-48701 | CVE-2022-48978 | CVE-2022-50050 | CVE-2022-50070 |
| • CVE-2022-50137 | CVE-2022-50228 | CVE-2022-50356 | CVE-2022-50367 |
| • CVE-2022-50386 | CVE-2022-50406 | CVE-2022-50408 | CVE-2023-53125 |
| • CVE-2023-53178 | CVE-2023-53185 | CVE-2023-53213 | CVE-2023-53226 |
| • CVE-2023-53232 | CVE-2023-53257 | CVE-2023-53305 | CVE-2023-53331 |
| • CVE-2023-53354 | CVE-2023-53373 | CVE-2023-53386 | CVE-2023-53401 |
| • CVE-2023-53494 | CVE-2024-28956 | CVE-2024-36350 | CVE-2024-36357 |
| • CVE-2024-46679 | CVE-2024-58240 | CVE-2025-22026 | CVE-2025-37797 |
| • CVE-2025-38498 | CVE-2025-38550 | CVE-2025-38556 | CVE-2025-38614 |
| • CVE-2025-38718 | CVE-2025-39682 | CVE-2025-39697 | CVE-2025-39702 |
| • CVE-2025-39718 | CVE-2025-39727 | CVE-2025-39730 | CVE-2025-39751 |
| • CVE-2025-39757 | CVE-2025-39817 | CVE-2025-39841 | CVE-2025-39849 |
| • CVE-2025-39864 | CVE-2025-39881 | CVE-2025-40300 | |

Bilan de la vulnérabilité

Redhat annonce la disponibilité de mises à jour permettant de corriger plusieurs vulnérabilités affectant le noyau de ses produits susmentionnés. L'exploitation de ces vulnérabilités peut permettre à un attaquant distant d'accéder à des données confidentielles, d'exécuter du code arbitraire, d'élever ses privilèges ou de causer un déni de service.

Solution

Veuillez se référer au bulletin de sécurité de Redhat afin d'installer les nouvelles mises à jour.

Risque

- Elévation de privilèges
- Accès à des données confidentielles
- Déni de service

Référence

Bulletin de sécurité de Redhat :

- <https://access.redhat.com/errata/RHSA-2025:19222>
- <https://access.redhat.com/errata/RHSA-2025:19223>
- <https://access.redhat.com/errata/RHSA-2025:19224>
- <https://access.redhat.com/errata/RHSA-2025:19268>
- <https://access.redhat.com/errata/RHSA-2025:19409>
- <https://access.redhat.com/errata/RHSA-2025:19440>
- <https://access.redhat.com/errata/RHSA-2025:19447>
- <https://access.redhat.com/errata/RHSA-2025:19469>
- <https://access.redhat.com/errata/RHSA-2025:19492>
- <https://access.redhat.com/errata/RHSA-2025:19886>
- <https://access.redhat.com/errata/RHSA-2025:19930>

- <https://access.redhat.com/errata/RHSA-2025:19932>
- <https://access.redhat.com/errata/RHSA-2025:19962>
- <https://access.redhat.com/errata/RHSA-2025:21051>
- <https://access.redhat.com/errata/RHSA-2025:21082>
- <https://access.redhat.com/errata/RHSA-2025:21083>
- <https://access.redhat.com/errata/RHSA-2025:21084>
- <https://access.redhat.com/errata/RHSA-2025:21091>
- <https://access.redhat.com/errata/RHSA-2025:21118>
- <https://access.redhat.com/errata/RHSA-2025:21128>
- <https://access.redhat.com/errata/RHSA-2025:21136>