Agence Nationale
des Systémes d'information
de l'état

Djibouti le, 11-06-2025

BULLETIN ALERTES

Object	Multiples vulnérabilités dans le noyau Linux de Red Hat
Réference	1353
Date de Publication	2025-06-06
Sévérité	Elevé

IMPACT :

- Atteinte à la confidentialité des données
- Déni de service
- Non spécifié par l'éditeur

SYSTÉME AFFECTÉ :

- Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 10.0 aarch64
- Red Hat CodeReady Linux Builder for ARM 64 10 aarch64
- Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 10.0 s390x
- Red Hat CodeReady Linux Builder for IBM z Systems 10 s390x
- Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 10.0 ppc64le
- Red Hat CodeReady Linux Builder for Power, little endian 10 ppc64le
- Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 10.0 x86_64
- Red Hat CodeReady Linux Builder for x86_64 10 x86_64
- Red Hat Enterprise Linux for ARM 64 - 4 years of updates 10.0 aarch64
- Red Hat Enterprise Linux for ARM 64 - Extended Update Support 10.0 aarch64
- Red Hat Enterprise Linux for ARM 64 10 aarch64
- 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 10.0 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 10.0 ppc64le
- Red Hat Enterprise Linux for Power, little endian 10 ppc64le
- 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 10.0 x86_64
- Red Hat Enterprise Linux for x86_64 10 x86_64

DÉSCRIPTION :

De nombreuses vulnérabilités ont été découvertes dans le noyau Linux de Red Hat. Elles permettent à un attaquant de provoquer une atteinte à la confidentialité des données, un déni de service et un problème de sécurité non spécifié par l'éditeur.

SOLUTION :

Consulter le bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

DOCUMENTATION :

- Bulletin de sécurité Red Hat RHSA-2025:8374 du 02 juin 2025

https://access.redhat.com/errata/RHSA-2025:8374

- Référence CVE CVE-2025-21919

https://www.cve.org/CVERecord?id=CVE-2025-21919

- Référence CVE CVE-2025-21964

https://www.cve.org/CVERecord?id=CVE-2025-21964

- Référence CVE CVE-2025-37785

https://www.cve.org/CVERecord?id=CVE-2025-37785