

Agence Nationale
des Systèmes d'information
de l'état

Djibouti le, 28-09-2024

BULLETIN ALERTES

Object	Multiples vulnérabilités dans le noyau Linux de Red Hat
Référence	1257
Date de Publication	2024-09-27
Sévérité	Critique

IMPACT :

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

SYSTÈME AFFECTÉ :

- Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.2 aarch64
- Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.4 aarch64
- Red Hat CodeReady Linux Builder for ARM 64 9 aarch64
- Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.2 s390x
- Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.4 s390x
- Red Hat CodeReady Linux Builder for IBM z Systems 9 s390x
- Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.2 ppc64le
- Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.4 ppc64le
- Red Hat CodeReady Linux Builder for Power, little endian 9 ppc64le
- Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.2 x86_64
- Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.4 x86_64
- Red Hat CodeReady Linux Builder for x86_64 9 x86_64
- 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 - Extended Update Support 9.2 aarch64
- Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.4 aarch64
- Red Hat Enterprise Linux for ARM 64 9 aarch64
- Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.4 s390x
- Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.2 s390x
- Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.4 s390x
- Red Hat Enterprise Linux for IBM z Systems 9 s390x
- Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.2 ppc64le
- Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.4 ppc64le
- Red Hat Enterprise Linux for Power, little endian 9 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 9 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 Real Time for NFV 9 x86_64
- 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 NFV for x86_64 - 4 years of updates 9.4 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 Real Time for x86_64 - 4 years of updates 9.4 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 - Extended Update Support 9.2 x86_64
- Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.4 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 - Update Services for SAP Solutions 8.6 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 9 x86_64
- Red Hat Enterprise Linux Server - AUS 7.7 x86_64
- Red Hat Enterprise Linux Server - AUS 8.4 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 - Extended Life Cycle Support (for IBM z Systems) 7 s390x
- Red Hat Enterprise Linux Server - Extended Life Cycle Support 7 x86_64
- Red Hat Enterprise Linux Server - Extended Life Cycle Support Extension (for IBM z Systems) 6 s390x
- Red Hat Enterprise Linux Server - Extended Life Cycle Support Extension 6 i386
- Red Hat Enterprise Linux Server - Extended Life Cycle Support Extension 6 x86_64
- Red Hat Enterprise Linux Server - Extended Life Cycle Support for IBM Power, big endian 7 ppc64
- Red Hat Enterprise Linux Server - Extended Life Cycle Support for IBM Power, little endian 7 ppc64le
- Red Hat Enterprise Linux Server - TUS 8.4 x86_64
- Red Hat Enterprise Linux Server - TUS 8.4 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 8.4 ppc64le
- 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 9.2 ppc64le
- Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.4 ppc64le

DÉSCRIPTION :

Plusieurs vulnérabilités ont été découvertes dans le noyau Linux de Red Hat. Certaines de ces failles permettent à un attaquant d'exécuter du code arbitraire à distance, d'obtenir une élévation de privilèges et de compromettre la confidentialité des données.

SOLUTION :

Mettre à jour le noyau Linux de Red Hat.(se référer à la documentation)

DOCUMENTATION :

- Bulletin de sécurité Red Hat RHSA-2024:6744 du 18 septembre 2024

<https://access.redhat.com/errata/RHSA-2024:6744>

- Bulletin de sécurité Red Hat RHSA-2024:6745 du 18 septembre 2024

<https://access.redhat.com/errata/RHSA-2024:6745>

- Bulletin de sécurité Red Hat RHSA-2024:6753 du 18 septembre 2024

<https://access.redhat.com/errata/RHSA-2024:6753>

- Bulletin de sécurité Red Hat RHSA-2024:6994 du 24 septembre 2024

<https://access.redhat.com/errata/RHSA-2024:6994>

- Bulletin de sécurité Red Hat RHSA-2024:6995 du 24 septembre 2024

<https://access.redhat.com/errata/RHSA-2024:6995>

- Bulletin de sécurité Red Hat RHSA-2024:6997 du 24 septembre 2024

<https://access.redhat.com/errata/RHSA-2024:6997>

- Bulletin de sécurité Red Hat RHSA-2024:6998 du 24 septembre 2024

<https://access.redhat.com/errata/RHSA-2024:6998>

- Bulletin de sécurité Red Hat RHSA-2024:6999 du 24 septembre 2024

<https://access.redhat.com/errata/RHSA-2024:6999>

- Bulletin de sécurité Red Hat RHSA-2024:7001 du 24 septembre 2024

<https://access.redhat.com/errata/RHSA-2024:7001>

- Bulletin de sécurité Red Hat RHSA-2024:7002 du 24 septembre 2024

<https://access.redhat.com/errata/RHSA-2024:7002>

- Bulletin de sécurité Red Hat RHSA-2024:7003 du 24 septembre 2024

<https://access.redhat.com/errata/RHSA-2024:7003>

- Bulletin de sécurité Red Hat RHSA-2024:7004 du 24 septembre 2024

<https://access.redhat.com/errata/RHSA-2024:7004>

- Bulletin de sécurité Red Hat RHSA-2024:7005 du 24 septembre 2024

<https://access.redhat.com/errata/RHSA-2024:7005>

- Bulletin de sécurité Red Hat RHSA-2024:7227 du 26 septembre 2024

<https://access.redhat.com/errata/RHSA-2024:7227>

- CVE-2021-46984

<https://www.cve.org/CVERecord?id=CVE-2021-46984>

- CVE-2021-47097

<https://www.cve.org/CVERecord?id=CVE-2021-47097>

- CVE-2021-47101

<https://www.cve.org/CVERecord?id=CVE-2021-47101>

- CVE-2021-47287

<https://www.cve.org/CVERecord?id=CVE-2021-47287>

- CVE-2021-47289

<https://www.cve.org/CVERecord?id=CVE-2021-47289>

- CVE-2021-47321

<https://www.cve.org/CVERecord?id=CVE-2021-47321>

- CVE-2021-47338

<https://www.cve.org/CVERecord?id=CVE-2021-47338>

- CVE-2021-47352

<https://www.cve.org/CVERecord?id=CVE-2021-47352>

- CVE-2021-47383

<https://www.cve.org/CVERecord?id=CVE-2021-47383>

- CVE-2021-47384

<https://www.cve.org/CVERecord?id=CVE-2021-47384>

- CVE-2021-47385

<https://www.cve.org/CVERecord?id=CVE-2021-47385>

- CVE-2021-47386

<https://www.cve.org/CVERecord?id=CVE-2021-47386>

- CVE-2021-47393

<https://www.cve.org/CVERecord?id=CVE-2021-47393>

- CVE-2021-47412

<https://www.cve.org/CVERecord?id=CVE-2021-47412>

- CVE-2021-47432

<https://www.cve.org/CVERecord?id=CVE-2021-47432>

- CVE-2021-47441

<https://www.cve.org/CVERecord?id=CVE-2021-47441>

- CVE-2021-47455

<https://www.cve.org/CVERecord?id=CVE-2021-47455>

- CVE-2021-47466

<https://www.cve.org/CVERecord?id=CVE-2021-47466>

- CVE-2021-47492

<https://www.cve.org/CVERecord?id=CVE-2021-47492>

- CVE-2021-47497

<https://www.cve.org/CVERecord?id=CVE-2021-47497>

- CVE-2021-47527

<https://www.cve.org/CVERecord?id=CVE-2021-47527>

- CVE-2021-47560

<https://www.cve.org/CVERecord?id=CVE-2021-47560>

- CVE-2021-47582

<https://www.cve.org/CVERecord?id=CVE-2021-47582>

- CVE-2021-47609

<https://www.cve.org/CVERecord?id=CVE-2021-47609>

- CVE-2022-48619

<https://www.cve.org/CVERecord?id=CVE-2022-48619>

- CVE-2022-48638

<https://www.cve.org/CVERecord?id=CVE-2022-48638>

- CVE-2022-48686

<https://www.cve.org/CVERecord?id=CVE-2022-48686>

- CVE-2022-48687

<https://www.cve.org/CVERecord?id=CVE-2022-48687>

- CVE-2022-48754

<https://www.cve.org/CVERecord?id=CVE-2022-48754>

- CVE-2022-48760

<https://www.cve.org/CVERecord?id=CVE-2022-48760>

- CVE-2022-48804

<https://www.cve.org/CVERecord?id=CVE-2022-48804>

- CVE-2022-48836

<https://www.cve.org/CVERecord?id=CVE-2022-48836>

- CVE-2022-48866

<https://www.cve.org/CVERecord?id=CVE-2022-48866>

- CVE-2023-52439

<https://www.cve.org/CVERecord?id=CVE-2023-52439>

- CVE-2023-52470

<https://www.cve.org/CVERecord?id=CVE-2023-52470>

- CVE-2023-52476

<https://www.cve.org/CVERecord?id=CVE-2023-52476>

- CVE-2023-52478

<https://www.cve.org/CVERecord?id=CVE-2023-52478>

- CVE-2023-52522

<https://www.cve.org/CVERecord?id=CVE-2023-52522>

- CVE-2023-52605

<https://www.cve.org/CVERecord?id=CVE-2023-52605>

- CVE-2023-52683

<https://www.cve.org/CVERecord?id=CVE-2023-52683>

- CVE-2023-52817

<https://www.cve.org/CVERecord?id=CVE-2023-52817>

- CVE-2023-52840

<https://www.cve.org/CVERecord?id=CVE-2023-52840>

- CVE-2023-52880

<https://www.cve.org/CVERecord?id=CVE-2023-52880>

- CVE-2023-52884

<https://www.cve.org/CVERecord?id=CVE-2023-52884>

- CVE-2023-6040

<https://www.cve.org/CVERecord?id=CVE-2023-6040>

- CVE-2024-2201

<https://www.cve.org/CVERecord?id=CVE-2024-2201>

- CVE-2024-23848

<https://www.cve.org/CVERecord?id=CVE-2024-23848>

- CVE-2024-26595

<https://www.cve.org/CVERecord?id=CVE-2024-26595>

- CVE-2024-26645

<https://www.cve.org/CVERecord?id=CVE-2024-26645>

- CVE-2024-26649

<https://www.cve.org/CVERecord?id=CVE-2024-26649>

- CVE-2024-26665

<https://www.cve.org/CVERecord?id=CVE-2024-26665>

- CVE-2024-26686

<https://www.cve.org/CVERecord?id=CVE-2024-26686>

- CVE-2024-26704

<https://www.cve.org/CVERecord?id=CVE-2024-26704>

- CVE-2024-26717

<https://www.cve.org/CVERecord?id=CVE-2024-26717>

- CVE-2024-26720

<https://www.cve.org/CVERecord?id=CVE-2024-26720>

- CVE-2024-26739

<https://www.cve.org/CVERecord?id=CVE-2024-26739>

- CVE-2024-26769

<https://www.cve.org/CVERecord?id=CVE-2024-26769>

- CVE-2024-26772

<https://www.cve.org/CVERecord?id=CVE-2024-26772>

- CVE-2024-26773

<https://www.cve.org/CVERecord?id=CVE-2024-26773>

- CVE-2024-26855

<https://www.cve.org/CVERecord?id=CVE-2024-26855>

- CVE-2024-26880

<https://www.cve.org/CVERecord?id=CVE-2024-26880>

- CVE-2024-26886

<https://www.cve.org/CVERecord?id=CVE-2024-26886>

- CVE-2024-26894

<https://www.cve.org/CVERecord?id=CVE-2024-26894>

- CVE-2024-26908

<https://www.cve.org/CVERecord?id=CVE-2024-26908>

- CVE-2024-26923

<https://www.cve.org/CVERecord?id=CVE-2024-26923>

- CVE-2024-26929

<https://www.cve.org/CVERecord?id=CVE-2024-26929>

- CVE-2024-26930

<https://www.cve.org/CVERecord?id=CVE-2024-26930>

- CVE-2024-26931

<https://www.cve.org/CVERecord?id=CVE-2024-26931>

- CVE-2024-26939

<https://www.cve.org/CVERecord?id=CVE-2024-26939>

- CVE-2024-26947

<https://www.cve.org/CVERecord?id=CVE-2024-26947>

- CVE-2024-26974

<https://www.cve.org/CVERecord?id=CVE-2024-26974>

- CVE-2024-26991

<https://www.cve.org/CVERecord?id=CVE-2024-26991>

- CVE-2024-26993

<https://www.cve.org/CVERecord?id=CVE-2024-26993>

- CVE-2024-27013

<https://www.cve.org/CVERecord?id=CVE-2024-27013>

- CVE-2024-27019

<https://www.cve.org/CVERecord?id=CVE-2024-27019>

- CVE-2024-27020

<https://www.cve.org/CVERecord?id=CVE-2024-27020>

- CVE-2024-27022

<https://www.cve.org/CVERecord?id=CVE-2024-27022>

- CVE-2024-27042

<https://www.cve.org/CVERecord?id=CVE-2024-27042>

- CVE-2024-35809

<https://www.cve.org/CVERecord?id=CVE-2024-35809>

- CVE-2024-35877

<https://www.cve.org/CVERecord?id=CVE-2024-35877>

- CVE-2024-35884

<https://www.cve.org/CVERecord?id=CVE-2024-35884>

- CVE-2024-35895

<https://www.cve.org/CVERecord?id=CVE-2024-35895>

- CVE-2024-35898

<https://www.cve.org/CVERecord?id=CVE-2024-35898>

- CVE-2024-35944

<https://www.cve.org/CVERecord?id=CVE-2024-35944>

- CVE-2024-35989

<https://www.cve.org/CVERecord?id=CVE-2024-35989>

- CVE-2024-36016

<https://www.cve.org/CVERecord?id=CVE-2024-36016>

- CVE-2024-36883

<https://www.cve.org/CVERecord?id=CVE-2024-36883>

- CVE-2024-36886

<https://www.cve.org/CVERecord?id=CVE-2024-36886>

- CVE-2024-36889

<https://www.cve.org/CVERecord?id=CVE-2024-36889>

- CVE-2024-36899

<https://www.cve.org/CVERecord?id=CVE-2024-36899>

- CVE-2024-36901

<https://www.cve.org/CVERecord?id=CVE-2024-36901>

- CVE-2024-36902

<https://www.cve.org/CVERecord?id=CVE-2024-36902>

- CVE-2024-36920

<https://www.cve.org/CVERecord?id=CVE-2024-36920>

- CVE-2024-36939

<https://www.cve.org/CVERecord?id=CVE-2024-36939>

- CVE-2024-36953

<https://www.cve.org/CVERecord?id=CVE-2024-36953>

- CVE-2024-37356

<https://www.cve.org/CVERecord?id=CVE-2024-37356>

- CVE-2024-38558

<https://www.cve.org/CVERecord?id=CVE-2024-38558>

- CVE-2024-38559

<https://www.cve.org/CVERecord?id=CVE-2024-38559>

- CVE-2024-38562

<https://www.cve.org/CVERecord?id=CVE-2024-38562>

- CVE-2024-38570

<https://www.cve.org/CVERecord?id=CVE-2024-38570>

- CVE-2024-38573

<https://www.cve.org/CVERecord?id=CVE-2024-38573>

- CVE-2024-38581

<https://www.cve.org/CVERecord?id=CVE-2024-38581>

- CVE-2024-38601

<https://www.cve.org/CVERecord?id=CVE-2024-38601>

- CVE-2024-38615

<https://www.cve.org/CVERecord?id=CVE-2024-38615>

- CVE-2024-38619

<https://www.cve.org/CVERecord?id=CVE-2024-38619>

- CVE-2024-39471

<https://www.cve.org/CVERecord?id=CVE-2024-39471>

- CVE-2024-39499

<https://www.cve.org/CVERecord?id=CVE-2024-39499>

- CVE-2024-39501

<https://www.cve.org/CVERecord?id=CVE-2024-39501>

- CVE-2024-39506

<https://www.cve.org/CVERecord?id=CVE-2024-39506>

- CVE-2024-40901

<https://www.cve.org/CVERecord?id=CVE-2024-40901>

- CVE-2024-40904

<https://www.cve.org/CVERecord?id=CVE-2024-40904>

- CVE-2024-40911

<https://www.cve.org/CVERecord?id=CVE-2024-40911>

- CVE-2024-40912

<https://www.cve.org/CVERecord?id=CVE-2024-40912>

- CVE-2024-40929

<https://www.cve.org/CVERecord?id=CVE-2024-40929>

- CVE-2024-40931

<https://www.cve.org/CVERecord?id=CVE-2024-40931>

- CVE-2024-40941

<https://www.cve.org/CVERecord?id=CVE-2024-40941>

- CVE-2024-40954

<https://www.cve.org/CVERecord?id=CVE-2024-40954>

- CVE-2024-40958

<https://www.cve.org/CVERecord?id=CVE-2024-40958>

- CVE-2024-40959

<https://www.cve.org/CVERecord?id=CVE-2024-40959>

- CVE-2024-40960

<https://www.cve.org/CVERecord?id=CVE-2024-40960>

- CVE-2024-40972

<https://www.cve.org/CVERecord?id=CVE-2024-40972>

- CVE-2024-40977

<https://www.cve.org/CVERecord?id=CVE-2024-40977>

- CVE-2024-40978

<https://www.cve.org/CVERecord?id=CVE-2024-40978>

- CVE-2024-40984

<https://www.cve.org/CVERecord?id=CVE-2024-40984>

- CVE-2024-40988

<https://www.cve.org/CVERecord?id=CVE-2024-40988>

- CVE-2024-40989

<https://www.cve.org/CVERecord?id=CVE-2024-40989>

- CVE-2024-40995

<https://www.cve.org/CVERecord?id=CVE-2024-40995>

- CVE-2024-40997

<https://www.cve.org/CVERecord?id=CVE-2024-40997>

- CVE-2024-40998

<https://www.cve.org/CVERecord?id=CVE-2024-40998>

- CVE-2024-41005

<https://www.cve.org/CVERecord?id=CVE-2024-41005>

- CVE-2024-41007

<https://www.cve.org/CVERecord?id=CVE-2024-41007>

- CVE-2024-41008

<https://www.cve.org/CVERecord?id=CVE-2024-41008>

- CVE-2024-41009

<https://www.cve.org/CVERecord?id=CVE-2024-41009>

- CVE-2024-41012

<https://www.cve.org/CVERecord?id=CVE-2024-41012>

- CVE-2024-41013

<https://www.cve.org/CVERecord?id=CVE-2024-41013>

- CVE-2024-41014

<https://www.cve.org/CVERecord?id=CVE-2024-41014>

- CVE-2024-41023

<https://www.cve.org/CVERecord?id=CVE-2024-41023>

- CVE-2024-41031

<https://www.cve.org/CVERecord?id=CVE-2024-41031>

- CVE-2024-41035

<https://www.cve.org/CVERecord?id=CVE-2024-41035>

- CVE-2024-41038

<https://www.cve.org/CVERecord?id=CVE-2024-41038>

- CVE-2024-41039

<https://www.cve.org/CVERecord?id=CVE-2024-41039>

- CVE-2024-41040

<https://www.cve.org/CVERecord?id=CVE-2024-41040>

- CVE-2024-41041

<https://www.cve.org/CVERecord?id=CVE-2024-41041>

- CVE-2024-41044

<https://www.cve.org/CVERecord?id=CVE-2024-41044>

- CVE-2024-41055

<https://www.cve.org/CVERecord?id=CVE-2024-41055>

- CVE-2024-41056

<https://www.cve.org/CVERecord?id=CVE-2024-41056>

- CVE-2024-41060

<https://www.cve.org/CVERecord?id=CVE-2024-41060>

- CVE-2024-41071

<https://www.cve.org/CVERecord?id=CVE-2024-41071>

- CVE-2024-41076

<https://www.cve.org/CVERecord?id=CVE-2024-41076>

- CVE-2024-41090

<https://www.cve.org/CVERecord?id=CVE-2024-41090>

- CVE-2024-41091

<https://www.cve.org/CVERecord?id=CVE-2024-41091>

- CVE-2024-41097

<https://www.cve.org/CVERecord?id=CVE-2024-41097>

- CVE-2024-42084

<https://www.cve.org/CVERecord?id=CVE-2024-42084>

- CVE-2024-42090

<https://www.cve.org/CVERecord?id=CVE-2024-42090>

- CVE-2024-42096

<https://www.cve.org/CVERecord?id=CVE-2024-42096>

- CVE-2024-42114

<https://www.cve.org/CVERecord?id=CVE-2024-42114>

- CVE-2024-42124

<https://www.cve.org/CVERecord?id=CVE-2024-42124>

- CVE-2024-42131

<https://www.cve.org/CVERecord?id=CVE-2024-42131>

- CVE-2024-42139

<https://www.cve.org/CVERecord?id=CVE-2024-42139>

- CVE-2024-42152

<https://www.cve.org/CVERecord?id=CVE-2024-42152>

- CVE-2024-42154

<https://www.cve.org/CVERecord?id=CVE-2024-42154>

- CVE-2024-42225

<https://www.cve.org/CVERecord?id=CVE-2024-42225>

- CVE-2024-42226

<https://www.cve.org/CVERecord?id=CVE-2024-42226>

- CVE-2024-42228

<https://www.cve.org/CVERecord?id=CVE-2024-42228>

- CVE-2024-42237

<https://www.cve.org/CVERecord?id=CVE-2024-42237>

- CVE-2024-42238

<https://www.cve.org/CVERecord?id=CVE-2024-42238>

- CVE-2024-42240

<https://www.cve.org/CVERecord?id=CVE-2024-42240>

- CVE-2024-42241

<https://www.cve.org/CVERecord?id=CVE-2024-42241>

- CVE-2024-42243

<https://www.cve.org/CVERecord?id=CVE-2024-42243>

- CVE-2024-42246

<https://www.cve.org/CVERecord?id=CVE-2024-42246>

- CVE-2024-42322

<https://www.cve.org/CVERecord?id=CVE-2024-42322>

- CVE-2024-43871

<https://www.cve.org/CVERecord?id=CVE-2024-43871>