



DJ-CERT

Centre national de veille,
d'alerte et de réponse aux
attaques informatiques

Autorité Nationale de Cybersécurité

Djibouti le, 14-02-2024

BULLETIN ALERTES

Objet	Multiples Vulnérabilités dans les produits Microsoft Windows
Référence	1108
Date de Publication	2024-02-14
Sévérité	Critique

IMPACT :

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

SYSTÈME AFFECTÉ :

- Windows Server 2019 (Server Core installation)
- Windows 10 Version 1809 for 32-bit Systems
- Windows 10 Version 1809 for x64-based Systems
- Windows Server 2022, 23H2 Edition (Server Core installation)
- Windows 11 Version 23H2 for x64-based Systems
- Windows Server 2022
- Windows 11 version 21H2 for x64-based Systems
- Windows 11 Version 23H2 for ARM64-based Systems
- Windows 10 Version 22H2 for 32-bit Systems
- Windows 10 Version 22H2 for ARM64-based Systems
- Windows Server 2019
- Windows 10 Version 22H2 for x64-based Systems
- Windows 11 Version 22H2 for x64-based Systems
- Windows 11 Version 22H2 for ARM64-based Systems
- Windows Server 2022 (Server Core installation)
- Windows 10 Version 21H2 for x64-based Systems
- Windows 10 Version 21H2 for ARM64-based Systems
- Windows 10 Version 21H2 for 32-bit Systems
- Windows 10 Version 1809 for ARM64-based Systems
- Windows 11 version 21H2 for ARM64-based Systems

DÉSCRIPTION :

Des nombreuses vulnérabilités ont été découvertes dans les systèmes Microsoft susmentionné. L'exploitation de ces vulnérabilités permet à un attaquant de provoquer un contournement de la fonctionnalité de sécurité, une atteinte à la confidentialité des données, un déni de service, une élévation de privilèges, une exécution de code arbitraire à distance et une usurpation d'identité.

NB : La faille CVE-2024-21412 est activement exploitée.

SOLUTION :

Appliquer les correctifs sur vos produit Microsoft Windows. (Se référer à la documentation)

DOCUMENTATION :

- Bulletin de sécurité Microsoft du 13 février 2024
<https://msrc.microsoft.com/update-guide/>
- CVE-2024-21355
<https://www.cve.org/CVERecord?id=CVE-2024-21355>
- CVE-2024-21354
<https://www.cve.org/CVERecord?id=CVE-2024-21354>
- CVE-2024-21349
<https://www.cve.org/CVERecord?id=CVE-2024-21349>
- CVE-2024-21348
<https://www.cve.org/CVERecord?id=CVE-2024-21348>
- CVE-2024-21405
<https://www.cve.org/CVERecord?id=CVE-2024-21405>
- CVE-2024-21391
<https://www.cve.org/CVERecord?id=CVE-2024-21391>
- CVE-2024-21412
<https://www.cve.org/CVERecord?id=CVE-2024-21412>
- CVE-2024-21343
<https://www.cve.org/CVERecord?id=CVE-2024-21343>
- CVE-2024-21406
<https://www.cve.org/CVERecord?id=CVE-2024-21406>
- CVE-2024-21366
<https://www.cve.org/CVERecord?id=CVE-2024-21366>
- CVE-2024-21365
<https://www.cve.org/CVERecord?id=CVE-2024-21365>
- CVE-2024-21362
<https://www.cve.org/CVERecord?id=CVE-2024-21362>
- CVE-2024-21361
<https://www.cve.org/CVERecord?id=CVE-2024-21361>
- CVE-2024-21360
<https://www.cve.org/CVERecord?id=CVE-2024-21360>
- CVE-2024-21370
<https://www.cve.org/CVERecord?id=CVE-2024-21370>
- CVE-2024-21359
<https://www.cve.org/CVERecord?id=CVE-2024-21359>
- CVE-2024-21356
<https://www.cve.org/CVERecord?id=CVE-2024-21356>
- CVE-2024-21368
<https://www.cve.org/CVERecord?id=CVE-2024-21368>
- CVE-2024-21352
<https://www.cve.org/CVERecord?id=CVE-2024-21352>
- CVE-2024-21351
<https://www.cve.org/CVERecord?id=CVE-2024-21351>
- CVE-2024-21371
<https://www.cve.org/CVERecord?id=CVE-2024-21371>
- CVE-2024-21358
<https://www.cve.org/CVERecord?id=CVE-2024-21358>
- CVE-2024-21357

- <https://www.cve.org/CVERecord?id=CVE-2024-21357>
- CVE-2024-21367
<https://www.cve.org/CVERecord?id=CVE-2024-21367>
- CVE-2024-21315
<https://www.cve.org/CVERecord?id=CVE-2024-21315>
- CVE-2024-21420
<https://www.cve.org/CVERecord?id=CVE-2024-21420>
- CVE-2024-21375
<https://www.cve.org/CVERecord?id=CVE-2024-21375>
- CVE-2024-21347
<https://www.cve.org/CVERecord?id=CVE-2024-21347>
- CVE-2024-21340
<https://www.cve.org/CVERecord?id=CVE-2024-21340>
- CVE-2024-21377
<https://www.cve.org/CVERecord?id=CVE-2024-21377>
- CVE-2024-21339
<https://www.cve.org/CVERecord?id=CVE-2024-21339>
- CVE-2024-21353
<https://www.cve.org/CVERecord?id=CVE-2024-21353>
- CVE-2024-20684
<https://www.cve.org/CVERecord?id=CVE-2024-20684>
- CVE-2023-50387
<https://www.cve.org/CVERecord?id=CVE-2023-50387>
- CVE-2024-21304
<https://www.cve.org/CVERecord?id=CVE-2024-21304>
- CVE-2024-21372
<https://www.cve.org/CVERecord?id=CVE-2024-21372>
- CVE-2024-21363
<https://www.cve.org/CVERecord?id=CVE-2024-21363>
- CVE-2024-21350
<https://www.cve.org/CVERecord?id=CVE-2024-21350>
- CVE-2024-21369
<https://www.cve.org/CVERecord?id=CVE-2024-21369>
- CVE-2024-21346
<https://www.cve.org/CVERecord?id=CVE-2024-21346>
- CVE-2024-21345
<https://www.cve.org/CVERecord?id=CVE-2024-21345>
- CVE-2024-21344
<https://www.cve.org/CVERecord?id=CVE-2024-21344>
- CVE-2024-21342
<https://www.cve.org/CVERecord?id=CVE-2024-21342>
- CVE-2024-21341
<https://www.cve.org/CVERecord?id=CVE-2024-21341>
- CVE-2024-21338
<https://www.cve.org/CVERecord?id=CVE-2024-21338>