DJ-CERT | Centre national de veille, d'alerte et de réponse aux attaques informatiques

Autorité Nationale de Cybersécurité

Djibouti le, 16-08-2024

BULLETIN ALERTES

Object	Vulnérabilité critique de RCE dans le protocole TCP/IP
Réference	1208
Date de Publication	2024-08-15
Sévérité	Critique

IMPACT :

- Exécution de code à distance

SYSTÉME AFFECTÉ :

- Microsoft Windows 10 Version 1809 32-bit Systems, x64-based Systems, ARM64-based Systems
  - Versions affectées : de 10.0.0 à 10.0.17763.6189
- Microsoft Windows Server 2019 x64-based Systems
  - Versions affectées : de 10.0.0 à 10.0.17763.6189
- Microsoft Windows Server 2019 (Server Core installation) x64-based Systems
  - Versions affectées : de 10.0.0 à 10.0.17763.6189
- Microsoft Windows Server 2022 x64-based Systems
  - Versions affectées : de 10.0.0 à 10.0.20348.2655
- Microsoft Windows 11 version 21H2 x64-based Systems, ARM64-based Systems
  - Versions affectées : de 10.0.0 à 10.0.22000.3147
- Microsoft Windows 10 Version 21H2 32-bit Systems, ARM64-based Systems
  - Versions affectées : de 10.0.0 à 10.0.19044.4780
- Microsoft Windows 11 version 22H2 ARM64-based Systems, x64-based Systems
  - Versions affectées : de 10.0.0 à 10.0.22621.4037

- Microsoft Windows 10 Version 22H2 x64-based Systems, ARM64-based Systems, 32-bit Systems
    - Versions affectées : de 10.0.0 à 10.0.19045.4780
- Microsoft Windows 11 version 22H3 ARM64-based Systems
    - Versions affectées : de 10.0.0 à 10.0.22631.4037
- Microsoft Windows 11 Version 23H2 x64-based Systems
    - Versions affectées : de 10.0.0 à 10.0.22631.4037
- Microsoft Windows Server 2022, 23H2 Edition (Server Core installation) x64-based Systems
    - Versions affectées : de 10.0.0 à 10.0.25398.1085
- Microsoft Windows 10 Version 1507 32-bit Systems, x64-based Systems
    - Versions affectées : de 10.0.0 à 10.0.10240.20751
- Microsoft Windows 10 Version 1607 32-bit Systems, x64-based Systems
    - Versions affectées : de 10.0.0 à 10.0.14393.7259
- Microsoft Windows Server 2016 x64-based Systems
    - Versions affectées : de 10.0.0 à 10.0.14393.7259
- Microsoft Windows Server 2016 (Server Core installation) x64-based Systems
    - Versions affectées : de 10.0.0 à 10.0.14393.7259
- Microsoft Windows Server 2008 Service Pack 2 32-bit Systems
    - Versions affectées : de 6.0.0 à 6.0.6003.22825
- Microsoft Windows Server 2008 Service Pack 2 (Server Core installation) 32-bit Systems, x64-based Systems
    - Versions affectées : de 6.0.0 à 6.0.6003.22825
- Microsoft Windows Server 2008 Service Pack 2 x64-based Systems
    - Versions affectées : de 6.0.0 à 6.0.6003.22825
- Microsoft Windows Server 2008 R2 Service Pack 1 x64-based Systems
    - Versions affectées : de 6.1.0 à 6.1.7601.27277
- Microsoft Windows Server 2008 R2 Service Pack 1 (Server Core installation) x64-based Systems
    - Versions affectées : de 6.0.0 à 6.1.7601.27277
- Microsoft Windows Server 2012 x64-based Systems
    - Versions affectées : de 6.2.0 à 6.2.9200.25031
- Microsoft Windows Server 2012 (Server Core installation) x64-based Systems
    - Versions affectées : de 6.2.0 à 6.2.9200.25031
- Microsoft Windows Server 2012 R2 x64-based Systems
    - Versions affectées : de 6.3.0 à 6.3.9600.22134
- Microsoft Windows Server 2012 R2 (Server Core installation) x64-based Systems
    - Versions affectées : de 6.3.0 à 6.3.9600.22134
- Microsoft Windows 11 Version 24H2 ARM64-based Systems, x64-based Systems
    - Versions affectées : de 10.0.0 à 10.0.26100.1457

DÉSCRIPTION :

Une vulnérabilité critique permettant l'exécution de code à distance (RCE) au sein du protocole TCP/IP. Cette faille touche tous les systèmes Windows qui utilisent IPv6, activé par défaut. Identifiée sous le code CVE-2024-38063, cette vulnérabilité résulte d'une faiblesse liée à un sous-dépassement d'entier (Integer Underflow). Les attaquants peuvent exploiter cette faille pour provoquer des dépassements de tampon, permettant ainsi l'exécution de code arbitraire sur les systèmes vulnérables, y compris Windows 10, Windows 11 et Windows Server.

CONTOURNEMENT PROVISOIRE :

- Microsoft recommande aux utilisateurs de désactiver IPv6 pour réduire la surface d'attaque, bien que cela puisse entraîner des dysfonctionnements de certains composants Windows.
- Il est fortement conseillé d'appliquer immédiatement les mises à jour de sécurité de Windows publiées cette semaine pour corriger cette vulnérabilité.
- Bloquer IPv6 via le pare-feu Windows ne suffit pas, car la vulnérabilité est exploitée avant le traitement par le pare-feu.

DOCUMENTATION :

- CVE-2024-38063

https://www.cve.org/CVERecord?id=CVE-2024-38063

- Avis de sécurité Microsoft

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38063