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

Autorité Nationale de Cybersécurité

Djibouti le, 05-05-2026

BULLETIN ALERTES

Object	Vulnérabilité Critique dans Microsoft Windows
Réference	1466
Date de Publication	2026-05-05
Sévérité	Critique

IMPACT :

- Élévation de privilèges
- Contournement de la politique de sécurité

SYSTÉME AFFECTÉ :

Windows 10 Version 22H2 for ARM64-based Systems

Windows 11 Version 24H2 for ARM64-based Systems

Microsoft Windows 11 23H2

Microsoft Windows 10 1607

Microsoft Windows 11

Microsoft Windows 10 21H2

Windows Server 2025 (Server Core installation)

Microsoft Windows Server 2012

Windows 10 Version 1809 for 32-bit Systems

Windows 11 Version 26H1 for ARM64-based Systems

Microsoft Windows 11 24h2

Windows 10 Version 21H2 for x64-based Systems

Microsoft Windows 10 22h2

Windows 11 version 26H1 for x64-based Systems

Microsoft Windows 10 1809

Windows 10 1607

Windows 10 Version 1607 for x64-based Systems

Windows Server 2022, 23H2 Edition (Server Core installation)

Windows 10 Version 22H2 for x64-based Systems

Windows 10 Version 21H2 for ARM64-based Systems

Windows 11 Version 25H2 for ARM systems

Microsoft Windows Server 2022

Microsoft Windows Server 2019

Microsoft Windows Server 2022 23h2

Windows Server 2012 R2 (Server Core installation)

Windows 11 Version 24H2 for x64-based Systems

Windows 11 Version 23H2 for ARM64-based Systems

Windows Server 2012 R2

Microsoft Windows

Microsoft Windows Server 2025

Microsoft Windows Server 2016

Windows Server 2012 Server Core Installation

Microsoft Windows 10

DÉSCRIPTION :

Il s’agit d’une vulnérabilité d’élévation de privilèges dans le composant Windows SMB Server de Microsoft.

Pour exploiter cette faille, l’attaquant doit d’abord disposer d’un accès local sur la machine cible avec un compte utilisateur standard (low privilege). Une fois cet accès obtenu, il interagit directement avec le serveur SMB local via localhost ou des named pipes. L’attaquant envoie alors des paquets SMB spécialement conçus pendant la phase de négociation de session et d’authentification. En raison d’un défaut de vérification dans le serveur SMB, celui-ci n’effectue pas correctement les contrôles sur le token d’authentification et les privilèges associés à la session. Cela permet à l’attaquant de forger ou de manipuler la session de manière à ce que le système lui attribue un token avec des privilèges beaucoup plus élevés, souvent jusqu’au niveau SYSTEM. Avec ce token élevé, l’attaquant peut alors exécuter des processus avec des droits administrateur complets, accéder aux fichiers système, modifier le registre, extraire des identifiants, désactiver les solutions de sécurité ou installer des malwares persistants. L’attaque est locale, ne nécessite aucune interaction utilisateur et fonctionne avec une complexité

SOLUTION :

Mettre à jour les systèmes affectés. (se référer à la documentation).

DOCUMENTATION :

Bulletin d’alerte Microsoft

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-26128