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

Autorité Nationale de Cybersécurité

Djibouti le, 14-05-2026

BULLETIN ALERTES

Object	Vulnérabilité Critique dans MSHTML Framework de Microsoft Windows
Réference	1470
Date de Publication	2026-05-14
Sévérité	Critique

IMPACT :

- Contournement de la politique de sécurité

SYSTÉME AFFECTÉ :

- **Windows 10** (toutes éditions)
  - Versions : 1507, 1607, 1809, 21H2, 22H2
  - Architectures : x86, x64, ARM64
- **Windows 11** (toutes éditions)
  - Versions : 21H2, 22H2, 23H2, 24H2, 25H2, 26H1
  - Architectures : x64, ARM64
- **Windows Server 2012 / 2012 R2**
  - Toutes versions (incluant Server Core)
- **Windows Server 2016**
  - Toutes versions
- **Windows Server 2019**
  - Toutes versions
- **Windows Server 2022**
  - Éditions : Standard, Datacenter, 23H2 (incluant Server Core)
- **Windows Server 2025**
  - Toutes versions (incluant Server Core)

Composant vulnérable

- **MSHTML Framework** — ieframe.dll (fonction _AttemptShellExecuteForHlinkNavigate)

DÉSCRIPTION :

CVE-2026-21513 est une vulnérabilité de type contournement de protection (CWE-693 — Protection Mechanism Failure) dans le composant MSHTML Framework de Microsoft Windows, spécifiquement dans la bibliothèque ieframe.dll.

Composant vulnérable : la fonction _AttemptShellExecuteForHlinkNavigate, responsable de la gestion de la navigation par hyperlien, ne valide pas suffisamment l'URL cible. Cette insuffisance de validation permet à une entrée contrôlée par l'attaquant d'atteindre des chemins de code qui invoquent ShellExecuteExW — permettant l'exécution de ressources locales ou distantes hors du contexte de sécurité du navigateur prévu.

Conditions d'exploitation : la victime doit ouvrir un fichier HTML ou LNK malveillant transmis par lien ou en pièce jointe email. Aucun privilège n'est requis de la part de l'attaquant. La complexité d'attaque est faible.

NB : Cette vulnérabilité a été exploitée comme zero-day. L'exploitation active est confirmée par Microsoft, CISA, Google.

SOLUTION :

Appliquer immédiatement la mise à jour de sécurité Microsoft du Patch Tuesday de Février 2026 sur l'ensemble des systèmes Windows (clients et serveurs).

DOCUMENTATION :

Références officielles et documentation :

• Advisory officiel Microsoft — CVE-2026-21513 Security Update Guide

• CISA KEV — Known Exploited Vulnerabilities Catalog

• Akamai — Analyse technique et IoCs APT28 — Inside the Fix: CVE-2026-21513

• The Hacker News — APT28 Tied to CVE-2026-21513 MSHTML 0-Day

• NVD — CVE-2026-21513 Detail