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

Autorité Nationale de Cybersécurité

Djibouti le, 18-04-2026

BULLETIN ALERTES

Object	Multiples vulnérabilités dans Microsoft Defender
Réference	1458
Date de Publication	2026-04-18
Sévérité	Elevé

IMPACT :

- Élévation de privilèges
- Déni de service
- Contournement des mécanismes de sécurité
- Compromission du système

SYSTÉME AFFECTÉ :

- Microsoft Defender version **4.0.0.0 antérieure à 4.18.26030.3011**

DÉSCRIPTION :

Plusieurs vulnérabilités ont été identifiées dans Microsoft Defender. Leur exploitation pourrait permettre à un attaquant, après un accès initial au système, d'élever ses privilèges jusqu'au niveau SYSTEM ou de provoquer un déni de service en bloquant les mises à jour de sécurité. Certaines de ces vulnérabilités sont activement exploitées et ne disposent pas encore de correctif, ce qui augmente significativement le risque global pour les systèmes affectés.

SOLUTION :

Appliquer immédiatement les mises à jour de sécurité disponibles (notamment pour CVE-2026-33825)

CONTOURNEMENT PROVISOIRE :

- Restreindre les privilèges utilisateurs
- Surveiller les comportements suspects (commandes système, élévation de privilèges)
- Isoler les systèmes compromis

DOCUMENTATION :

CVE-2026-33825 :

- https://www.cve.org/CVERecord?id=CVE-2026-33825