AVIS DE SECURITE

Objet	Vulnérabilités importantes d'exécution de code à distance et d'élévation de privilèges dans Microsoft Edge
Niveau de criticité	**IMPORTANT**
Référence	SNCSIRT-2026-ADS-210
TLP	WHITE

Résumé

Microsoft a publié le 15 septembre 2026 des correctifs pour deux vulnérabilités importantes affectant Microsoft Edge (Chromium) : CVE-2026-69486, un débordement de tampon en tas (CWE-122, CVSS 8.8) permettant une exécution de code arbitraire à distance lorsque l'utilisateur ouvre un fichier spécialement conçu, et CVE-2026-85893, une utilisation de mémoire libérée (use-after-free, CWE-416, CVSS 8.8) permettant une élévation de privilèges après deux gestes tactiles déclenchant l'auto-remplissage sur une page web contrôlée par l'attaquant. Ces deux vulnérabilités, spécifiques à Edge, sont distinctes des CVE Chromium/V8 déjà couvertes par les bulletins Chrome (SNCSIRT-2026-ADS-180/199/209) ; Microsoft ne signale aucune exploitation active à ce jour.

Risque de sécurité

- Exécution de code arbitraire à distance (CVE-2026-69486, CVSS 8.8, débordement de tampon en tas)
- Élévation de privilèges (CVE-2026-85893, CVSS 8.8, use-after-free)

Systèmes affectés

- Microsoft Edge (Chromium) versions antérieures à 153.0.4234.32

Recommandations

Se référer au bulletin de sécurité de l'éditeur du 15 septembre 2026 :

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-69486
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-85893