AVIS DE SECURITE

Objet	Vulnérabilité critique de contournement de liste d'autorisation de désérialisation dans Apache MINA (branches 2.0.x et 2.1.x)
Niveau de criticité	**CRITIQUE**
Référence	SNCSIRT-2026-ADS-219
TLP	WHITE

Résumé

La fondation Apache a divulgué le 21 septembre 2026 la vulnérabilité CVE-2026-94301 (CVSS 9.8) affectant la bibliothèque réseau Java Apache MINA. Le correctif de CVE-2026-47065 (surcharge de resolveProxyClass() empêchant le contournement de la liste d'autorisation acceptMatchers via des objets java.lang.reflect.Proxy), annoncé comme complet en juin 2026, n'avait en réalité été appliqué qu'à la branche 2.2.x. Les branches 2.0.x et 2.1.x restent donc vulnérables à un contournement du filtre de désérialisation pouvant mener à l'exécution de code arbitraire dans les applications utilisant ObjectSerializationDecoder pour traiter des données non fiables. Aucune exploitation active n'est signalée à ce jour.

Risque de sécurité

- Exécution de code arbitraire à distance (CVE-2026-94301, CVSS 9.8)
- Contournement de la politique de sécurité (liste d'autorisation de désérialisation)
- Atteinte à la confidentialité et à l'intégrité des données

Systèmes affectés

- Apache MINA 2.0.0 à 2.0.30
- Apache MINA 2.1.0 à 2.1.14
- Applications utilisant IoBuffer#getObject() / ObjectSerializationCodecFactory dans la chaîne de filtres (FtpServer, SSHD et Vysper ne sont pas concernés selon l'éditeur)

Recommandations

1. Se référer au bulletin de sécurité de l'éditeur du 21 septembre 2026 :
   - https://mina.apache.org/mina-project/news (annonces de sécurité Apache MINA)
   - https://www.cve.org/CVERecord?id=CVE-2026-94301 (fiche CVE)
2. Mettre à niveau vers Apache MINA 2.0.31, 2.1.15 ou 2.2.8 et ultérieur, puis vérifier que seules les classes strictement nécessaires sont autorisées dans ObjectSerializationDecoder
3. Recenser les applications et produits tiers embarquant Apache MINA 2.0.x/2.1.x et suivre les correctifs de leurs éditeurs