



BULLETIN DE SECURITE

Titre	Vulnérabilités critiques dans des plugins WordPress
Numéro de Référence	58722511/25
Date de Publication	25 Novembre 2025
Risque	Critique
Impact	Critique

Systèmes affectés

- Edukart-pro 1.0.3 et version antérieure,
- sneeit-framework 8.4 et version antérieure,
- elex-helpdesk-customer-support-ticket-system 3.3.1 et version antérieure.

Identificateurs externes

- CVE-2025-13559, CVE-2025-6389, CVE-2025-11456

Bilan de la vulnérabilité

WordPress a signalé plusieurs vulnérabilités critiques permettant à des acteurs malveillants non authentifiés d'exploiter des failles d'élévation de privilèges, d'exécution de code à distance et d'upload arbitraire de fichiers, facilitant ainsi l'injection de web shells ou de payloads persistants. Ces vecteurs d'attaque exposent les sites concernés à une compromission totale. Le niveau de risque est critique, imposant une mise à jour immédiate ou la désactivation des extensions vulnérables.

Solution

- Veuillez se référer au bulletin de sécurité WordPress afin d'installer les nouvelles mises à jour ;
- Aucun correctif n'est actuellement disponible pour « Edukart-pro ». Veuillez examiner en détail les informations relatives à la vulnérabilité et appliquer des mesures de mitigation adaptées au niveau de tolérance au risque de votre organisation. Il peut être préférable de désinstaller le plugin concerné et d'envisager une solution de remplacement.

Risque

- Exécution du code arbitraire à distance,
- Elévation de privilèges,

- Accès aux informations confidentielles,
- Upload de fichiers malveillants,
- Compromission de site web.

Annexe

Bulletins de sécurité WordPress:

- <https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/edukart-pro-2/edukart-pro-103-unauthenticated-privilege-escalation>
- <https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/sneet-framework/sneet-framework-83-unauthenticated-remote-code-execution-in-sneet-articles-pagination-callback>
- <https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/elex-helpdesk-customer-support-ticket-system/elex-wordpress-helpdesk-customer-ticketing-system-331-unauthenticated-arbitrary-file-upload>