ROYAUME DU MAROC
ADMINISTRATION
DE LA DEFENSE NATIONALE
Direction Générale de la Sécurité des Systèmes d'Information
Centre de Veille de Détection et de Réaction aux Attaques Informatiques

المملكة المغربية
إدارة الدفاع الوطني
المديرية العامة لأمن نظم المعلومات
مركز اليقظة والرصد والتصدي للهجمات المعلوماتية

BULLETIN DE SECURITE

Titre	Vulnérabilités affectant Logpoint
Numéro de Référence	58802811/25
Date de publication	28Novembre 2025
Risque	Important
Impact	Important

Systèmes affectés

- Logpoint versions antérieures à la version 7.7.0.

Identificateurs externes

- CVE-2025-66359 CVE-2025-66360 CVE-2025-66361

Bilan de la vulnérabilité

Trois vulnérabilités affectant les versions susmentionnées de Logpoint ont été corrigées. L'exploitation de ces vulnérabilités peut permettre à un attaquant distant d'injecter du contenu dans une page, d'élever ses privilèges ou d'accéder à des informations confidentielles.

Solution

Veuillez se référer aux bulletins de sécurité de Cisco pour mettre à jours vos produits.

Direction Générale de la Sécurité des Systèmes d'Information,
Centre de Veille de Détection et de Réaction aux Attaques Informatiques
Tél : 05 37 57 21 47 – Fax : 05 37 57 20 53
Email : contact@macert.gov.ma

المديرية العامة لأمن نظم المعلومات ,مديرية تدبير مركز اليقظة والرصد والتصدي للهجمات المعلوماتية
هاتف: 47 21 57 37 05 – فاكس: 53 20 57 37 05
البريد الإلكتروني contact@macert.gov.ma

Risques

- Injection de contenu dans une page
- Elévation de privilèges
- Accès à des informations confidentielles

Références

Bulletins de sécurité de Cisco :

- https://servicedesk.logpoint.com/hc/en-us/articles/29158899698333-XSS-Vulnerability-due-to-insufficient-input-validation
- https://servicedesk.logpoint.com/hc/en-us/articles/29160917867549-Redis-communication-exposed-for-internal-communication
- https://servicedesk.logpoint.com/hc/en-us/articles/29160993806749-Process-Data-Exposure-Under-High-Load