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 critiques affectant des produits de Cisco
Numéro de Référence	58120711/25
Date de publication	07 Novembre 2025
Risque	Important
Impact	Critique

Systèmes affectés

- Cisco Identity Services Engine versions 3.4 antérieures à 3.4 patch 4
- Cisco Identity Services Engine versions 3.3 antérieures à 3.4 patch 8
- Cisco Identity Services Engine versions 3.2 antérieures à 3.4 patch
- Cisco Identity Services Engine versions 3.1
- Unified CCX versions 15.x antérieures à 15.0 ES01
- Unified CCX versions antérieures à 12.5 SU3 ES07
- Cisco Secure Firewall Adaptive Security Appliance Software versions antérieures à 9.12.4.72, 9.14.4.28, 9.16.4.23, 9.18.4.19 et 9.20.2
- IOS Software et IOS XE
- IOS XR Software
- Secure Firewall Threat Defense Software versions antérieures à 6.6.7.2, 7.0.6, 7.2.6 et 7.4.2 and later

Identificateurs externes

- CVE-2025-20362 CVE-2025-20363 CVE-2025-20333 CVE-2025-20374
- CVE-2025-20375 CVE-2025-20376 CVE-2025-20377 CVE-2025-20289
- CVE-2025-20303 CVE-2025-20304 CVE-2025-20305 CVE-2025-20343

Bilan de la vulnérabilité

Cisco annonce la correction de plusieurs vulnérabilités critiques affectant certaines versions de ses produits susmentionnés. Une de ces vulnérabilités identifiée par « CVE-2025-20333 » est activement exploitée. L'exploitation de ces vulnérabilités peut permettre à un attaquant distant d'injecter du contenu dans une page, d'exécuter du code, de contourner des mesures de sécurité ou de causer un déni de service.

Solution

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

Risques

- Injection de contenu dans une page
- Exécution de code à distance
- Contournement de mesures de sécurité
- Déni de service

Références

Bulletins de sécurité de Cisco :

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-webvpn-YROOTUW
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-http-code-exec-WmfP3h3O
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-webvpn-z5xP8EUB
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cc-mult-vuln-gK4TFXSn
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-multiple-vulns-O9BESWJH
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-radsupress-dos-8YF3JThh

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: 05 37 57 21 47 – فاكس: 05 37 57 20 53
البريد الإلكتروني contact@macert.gov.ma