ROYAUME DU MAROC
ADMINISTRATION
DE LA DEFENSE NATIONALE
Direction Générale de la Sécurité des Systèmes d'Information

المملكة المغربية
إدارة الدفاع الوطني
المديرية العامة لأمن نظم المعلومات

BULLETIN DE SECURITE

Titre	Vulnérabilités critiques dans les produits Cisco
Numéro de Référence	63271604/26
Date de Publication	16 Avril 2026
Risque	Critique
Impact	Critique

Systèmes affectés

- Cisco ISE versions 3.2 antérieures à 3.2 Patch 8
- Cisco ISE versions 3.3 antérieures à 3.3 Patch 8
- Cisco ISE versions 3.4 antérieures à 3.4 Patch 4
- Cisco ISE versions 3.5 antérieures à 3.5 Patch 3
- Cisco ISE/ISE-PIC versions 3.1 antérieures à 3.1 Patch 11(avril 2026)
- Cisco ISE/ISE-PIC versions 3.2 antérieures à 3.2 Patch 10(avril 2026)
- Cisco ISE/ISE-PIC versions 3.3 antérieures à 3.3 Patch 11(avril 2026)
- Cisco ISE/ISE-PIC versions 3.4 antérieures à 3.4 Patch 6 (avril 2026)
- Cisco Webex Services version 39.x antérieure ou égale 39.11
- Cisco Webex Services version 40.x antérieure ou égale 40.6.2
- Cisco Webex Services version 42.x antérieure ou égale 42.12
- Cisco Webex Services version 43.x antérieure ou égale 43.12
- Cisco Webex Services version 44.x antérieure ou égale 44.12
- Cisco Webex Services version 45.x antérieure ou égale 45.4
- Cisco AsyncOS Software pour Cisco Secure Web Appliance versions 15.2.x

Identificateurs externes

- CVE-2026-20184 CVE-2026-20147 CVE-2026-20148 CVE-2026-20180 CVE-2026-20186
- CVE-2026-20152 CVE-2026-20170 CVE-2026-20059 CVE-2026-20060 CVE-2026-20078
- CVE-2026-20081 CVE-2026-20161 CVE-2026-20132 CVE-2026-20136 CVE-2026-20060
- CVE-2026-20061

Bilan de la vulnérabilité

Cisco annonce avoir corrigé plusieurs vulnérabilités critiques affectant les produits, susmentionnés. L'exploitation de ces vulnérabilités pourrait permettre à un attaquant distant ou authentifié disposant d'un accès réseau ou local d'exécuter des commandes arbitraires, de contourner l'authentification, d'obtenir un contrôle administratif complet sur l'équipement,

de causer un déni de service, d'écrire des fichiers arbitraires et d'injecter du code malveillant via des interfaces web vulnérables, ce qui compromette la confidentialité, l'intégrité et la disponibilité des systèmes affectés.

Solution

Veuillez se référer au bulletin de sécurité Cisco du 15 Avril 2026 pour plus d'information.

Risque

- Déni de service ;
- Élévation de privilèges ;
- Injection de code indirecte à distance (XSS) ;
- Injection de commandes ;
- Elévation de privilèges ;
- Contournement d'authentification ;
- Écriture de fichiers arbitraires ;
- Atteinte à la confidentialité des données ;
- Atteinte à l'intégrité des données ;

Annexe

Bulletin de sécurité Cisco du 15 Avril 2026:

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-rce-4fverepv
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-cui-cert-8jSZYhWL
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-rce-traversal-8bYndVrZ#fs
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wsa-auth-bypass-6YZkTQhd
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webexcc-xss-WEX5nUnA
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-unity-vulns-n2EJSbbw
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-unity-file-download-RmKEVWPx
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-te-agentfilewrite-tqUw3SMU
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-cmd-inj-5WSJcYJB