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	62750204/26
Date de Publication	02 Avril 2026
Risque	Critique
Impact	Critique

Systèmes affectés

- Cisco SSM On-Prem version antérieure à 9-202601 ;
- Cisco Integrated Management Controller (IMC) version 4.15.x antérieure à 4.15.6 ;
- Cisco Integrated Management Controller (IMC) version 4.18.x antérieure à 4.18.3 ;
- Nexus Dashboard versions 3.2 et 4.1 antérieure à 4.2 ;
- Nexus Dashboard Insights versions antérieure à 6.5 ;
- Cisco Evolved Programmable Network Manager version antérieure à EPNM 8.1.2 ;

Identificateurs externes

- CVE-2026-20041 CVE-2026-20042 CVE-2026-20085 CVE-2026-20087 CVE-2026-20088 ;
- CVE-2026-20089 CVE-2026-20090 CVE-2026-20093 CVE-2026-20094 CVE-2026-20095 ;
- CVE-2026-20096 CVE-2026-20097 CVE-2026-20155 CVE-2026-20160 CVE-2026-20174 ;

Bilan de la vulnérabilité

Cisco annonce avoir corrigé plusieurs vulnérabilités critiques affectant ses produits, notamment Cisco Smart Software Manager On-Prem, Cisco Integrated Management Controller, Cisco Nexus Dashboard et Cisco Evolved Programmable Network Manager. 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 avec les privilèges « root », 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 01 Avril 2026 pour plus d'information.

Direction Générale de la Sécurité des Systèmes d'Information,
Centre de Veille de Détection et de Réaction aux Attaques Informatiques, Méchouar Saïd,
B.P. 1048 Rabat – 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 ، المشور السعيد، ص.ب. 1048 الرباط
هاتف: 47 21 57 37 05 – فاكس: 53 20 57 37 05
البريد الإلكتروني contact@macert.gov.ma

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 01 Avril 2026:

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ssm-cli-execution-cHUcWuNr
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-auth-bypass-AgG2BxTn
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-epnm-improp-auth-mUwFWUU3
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cssm-priv-esc-xRAnOuO8
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-cmd-inj-3hKN3bVt
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ndi-afw-rJuRC5dZ
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nd-ssrf-NAen4O7r
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nd-cbid-5YqkOSHu
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-xss-A2tkgVAB

Direction Générale de la Sécurité des Systèmes d'Information,
Centre de Veille de Détection et de Réaction aux Attaques Informatiques, Méchouar Saïd,
B.P. 1048 Rabat – 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 ، المشور السعيد، ص.ب. 1048 الرباط
هاتف: 05 37 57 21 47 – فاكس: 05 37 57 20 53
البريد الإلكتروني contact@macert.gov.ma