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 des produits de Cisco
Numéro de Référence	50462410/24
Date de publication	24 Octobre 2024
Risque	Important
Impact	Critique

Systèmes affectés

- Cisco Secure Firewall Management Center Software
- Cisco Adaptive Security Appliance Software
- Cisco Firepower Threat Defense Software for Firepower 1000, 2100, 3100, and 4200 Series
- Cisco Firepower Threat Defense Software for Cisco Firepower 2100 Series
- Cisco Adaptive Security Appliance and Firepower Threat Defense Software
- Cisco Firepower Threat Defense Software and Cisco FirePOWER Services
- Cisco Adaptive Security Virtual Appliance and Secure Firewall Threat Defense
- Cisco Adaptive Security Appliance and Firepower Threat Defense Software
- Cisco Secure Firewall Management Center
- Cisco Adaptive Security Appliance and Firepower Threat Defense Software
- Cisco Firepower Threat Defense Software
- Cisco Secure Client

Identificateurs externes

CVE-2024-20260, CVE-2024-20264, CVE-2024-20269, CVE-2024-20273, CVE-2024-20298, CVE-2024-20300, CVE-2024-20364, CVE-2024-20372, CVE-2024-20386, CVE-2024-20403, CVE-2024-20409, CVE-2024-20410, CVE-2024-20415, CVE-2024-20268, CVE-2024-20274, CVE-2024-20275, CVE-2024-20297, CVE-2024-20299, CVE-2024-20329, CVE-2024-20330, CVE-2024-20331, CVE-2024-20339, CVE-2024-20340, CVE-2024-20341, CVE-2024-20382, CVE-2024-20342, CVE-2024-20351, CVE-2024-20370, CVE-2024-20374, CVE-2024-20377, CVE-2024-20387, CVE-2024-20388, CVE-2024-20379, CVE-2024-20384, CVE-2024-20402, CVE-2024-20407, CVE-2024-20408, CVE-2024-20412, CVE-2024-20424, CVE-2024-20426,

CVE-2024-20431, CVE-2024-20471, CVE-2024-20472, CVE-2024-20473, CVE-2024-20474, CVE-2024-20481, CVE-2024-20482, CVE-2024-20485, CVE-2024-20493, CVE-2024-20494, CVE-2024-20495, CVE-2024-20526

Bilan de la vulnérabilité

Cisco annonce la correction de plusieurs vulnérabilités affectant certaines versions de ses produits susmentionnés. Trois de ces vulnérabilités identifiées par «CVE-2024-20412 », « CVE-2024-20424 » et « CVE-2024-20329 » sont critiques. L'exploitation de ces vulnérabilités peut permettre à un attaquant distant d'exécuter du code, d'accéder à des données confidentielles, d'injecter du code SQL, de contourner des mesures de sécurité, d'élever ses privilèges ou de causer un déni de service.

Solution

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

Risques

- Exécution de code à distance
- Accès à des données confidentielles
- Injection de code SQL
- Contournement de mesures de sécurité
- Elévation de privilèges
- Déni de service

Références

Bulletins de sécurité de Cisco :

- https://seccloudappsciscocom/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-ftd-priv-esc-hBS9gnwq
- https://seccloudappsciscocom/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-ssh-dos-eEDWu5RM
- https://seccloudappsciscocom/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-ssh-rce-gRAuPEUF
- https://seccloudappsciscocom/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-tls-CWY6zXB

- https://seccloudappsciscocom/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-vpn-4gYEWMKg
- https://seccloudappsciscocom/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-vpn-cZf8gT
- https://seccloudappsciscocom/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-vpn-nyH3fhp
- https://seccloudappsciscocom/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-acl-bypass-VvnLNKqf
- https://seccloudappsciscocom/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-bf-dos-vDZhLqrW
- https://seccloudappsciscocom/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-dap-dos-bhEkP7n
- https://seccloudappsciscocom/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-ikev2-dos-9FgEyHsF
- https://seccloudappsciscocom/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-nsgacl-bypass-77XnEAsL
- https://seccloudappsciscocom/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-lce-vU3ekMJ3
- https://seccloudappsciscocom/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-snmp-dos-7TcnzxTU
- https://seccloudappsciscocom/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-webvpn-dos-hOnB9pH4
- https://seccloudappsciscocom/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-xss-yjj7ZjVq
- https://seccloudappsciscocom/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdvirtual-dos-MuenGnYR
- https://seccloudappsciscocom/security/center/content/CiscoSecurityAdvisory/cisco-sa-csc-dos-XvPhM3bj
- https://seccloudappsciscocom/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-cmd-inj-2HBkA97G
- https://seccloudappsciscocom/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-cmd-inj-g8AOKnDP
- https://seccloudappsciscocom/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-cmd-inj-v3AWDqN7
- https://seccloudappsciscocom/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-file-read-5q4mQRn
- https://seccloudappsciscocom/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-html-inj-nfJeYHxz

- https://seccloudappsciscocom/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-priv-esc-CMQ4S6m7
- https://seccloudappsciscocom/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-sql-inj-LOYAFcfq
- https://seccloudappsciscocom/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-sql-inject-2EnmTC8v
- https://seccloudappsciscocom/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-xss-dhJxQYZs
- https://seccloudappsciscocom/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-xss-infodisc-RL4mJFer
- https://seccloudappsciscocom/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-geoip-bypass-MB4zRDu
- https://seccloudappsciscocom/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-statcred-dFC8tXT5
- https://seccloudappsciscocom/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-tls-dos-QXYE5Ufy
- https://seccloudappsciscocom/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-vdb-snort-djj4cnbR
- https://seccloudappsciscocom/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd2100-snort-dos-M9HuMt75
- https://seccloudappsciscocom/security/center/content/CiscoSecurityAdvisory/cisco-sa-sa-ftd-snort-fw-BCJTZPMu
- https://seccloudappsciscocom/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-bypass-PTry37fX
- https://seccloudappsciscocom/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-rf-bypass-OY8f3pnM