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 plusieurs produits de cisco
Numéro de Référence	41190704/23
Date de publication	07 Avril 2023
Risque	Important
Impact	Critique

Systèmes affectés

- Cisco Secure Network Analytics versions antérieures à 7.4.1-PATCH SMC Rollup #5
- Cisco Small Business RV320 et RV325 Dual Gigabit WAN VPN Routers
- Cisco EPNM versions antérieures à 7.0.1
- Cisco ISE versions 3.2 antérieures à 3.2P1
- Cisco Prime Infrastructure versions antérieures à 3.10.4
- Cisco Expressway Series et Cisco TelePresence VCS versions antérieures à 14.3
- Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers
- Cisco Duo Authentication for macOS and Duo Authentication for Windows
- Cisco Packet Data Network Gateway
- Cisco Webex Meetings Web UI
- Cisco Secure Network Analytics
- Cisco Unified Contact Center Express
- Cisco Meraki

Identificateurs externes

CVE-2022-20812 CVE-2022-20813 CVE-2023-02121 CVE-2023-20102
CVE-2023-20117 CVE-2023-20121 CVE-2023-20122 CVE-2023-20128
CVE-2023-20127 CVE-2023-20129 CVE-2023-20130 CVE-2023-20131
CVE-2023-20124 CVE-2023-20152 CVE-2023-20153 CVE-2023-20137
CVE-2023-20138 CVE-2023-20139 CVE-2023-20140 CVE-2023-20141
CVE-2023-20142 CVE-2023-20143 CVE-2023-20144 CVE-2023-20145

CVE-2023-20146 CVE-2023-20147 CVE-2023-20148 CVE-2023-20149
CVE-2023-20150 CVE-2023-20151 CVE-2023-20123 CVE-2023-20051
CVE-2023-20132 CVE-2023-20134 CVE-2023-20103 CVE-2023-20096

Bilan de la vulnérabilité

Cisco annonce la correction de plusieurs vulnérabilités affectant certaines versions de ses produits susmentionnés. L'exploitation de ces vulnérabilités peut permettre à un attaquant distant d'exécuter du code arbitraire, de contourner des mesures de sécurité ou d'accéder à des données confidentielles.

Solution

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

Risques

- Exécution de code arbitraire
- Contournement de mesures de sécurité
- Accès à des données confidentielles

Références

Bulletins de sécurité de Cisco :

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-stealthsmc-rce-sfNBPjcS
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-adeos-MLAyEcvk
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv32x-cmdinject-cKQsZpxL
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-pi-epnm-eRPWAXLe
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv01x_rv32x_rce-nzAGWWDD
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-injection-2XbOg9Dg

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

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-pdng-dos-KmzwEy2Q
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-duo-replay-knuNKd
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-stealth-rce-BDwXFK9C
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-uccx-xss-GO9L9xxr
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-lsp-7xySn6pj