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	40492302 /23
Date de Publication	23 Février 2023
Risque	Critique
Impact	Critique

Systèmes affectés

- Secure Endpoint, formerly Advanced Malware Protection (AMP) pour Endpoints, pour Linux
- Secure Endpoint, formerly Advanced Malware Protection (AMP) pour Endpoints, pour MacOS
- Secure Endpoint, formerly Advanced Malware Protection (AMP) pour Endpoints, pour Windows
- Secure Endpoint Private Cloud
- Secure Web Appliance, formerly Web Security Appliance
- Cisco APIC
- Cisco Cloud Network Controller
- Cisco Nexus 9000 Series Fabric Switches
- Firepower 4100 Series
- Firepower 9300 Security Appliances
- UCS 6200 Series Fabric Interconnects
- UCS 6300 Series Fabric Interconnects
- UCS 6400 Series Fabric Interconnects
- UCS 6500 Series Fabric Interconnects
- MDS 9000 Series Multilayer Switches (CSCwd18009)
- Nexus 1000 Virtual Edge pour VMware vSphere (CSCwd18012)
- Nexus 1000V Switch pour Microsoft Hyper-V (CSCwd18012)
- Nexus 1000V Switch pour VMware vSphere (CSCwd18012)

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

- Nexus 3000 Series Switches (CSCwd00653)
- Nexus 5500 Platform Switches (CSCwd18013)
- Nexus 5600 Platform Switches (CSCwd18013)
- Nexus 6000 Series Switches (CSCwd18013)
- Nexus 7000 Series Switches (CSCwd18011)
- Nexus 9000 Series Switches in standalone NX-OS mode (CSCwd00653)
- Firepower 4100 Series
- Firepower 9300 Security Appliances
- UCS 6200 Series Fabric Interconnects
- UCS 6300 Series Fabric Interconnects
- UCS 6400 Series Fabric Interconnects
- UCS 6500 Series Fabric Interconnects
- N9K-C93180YC-FX3
- N9K-C93180YC-FX3S

Identificateurs externes

- CVE-2023-20032, CVE-2023-20011, CVE-2023-20089, CVE-2023-20016, CVE-2023-20050, CVE-2023-20015, CVE-2023-20012

Bilan de la vulnérabilité

Plusieurs vulnérabilités critiques ont été corrigées dans les produits Cisco susmentionnés. Un attaquant pourrait exploiter ces failles afin d'exécuter du code arbitraire à distance, réussir une élévation de privilèges, causer un déni de service, contourner la politique de sécurité ou porter atteinte à la confidentialité de données.

Solution

Veuillez se référer au bulletin de sécurité Cisco du 22 Février 2023 pour plus d'information.

Risque

- Exécution de code arbitraire à distance
- Elévation de privilèges
- Déni de service
- Contournement de la politique de sécurité
- Atteinte à la confidentialité de données

Annexe

Bulletins de sécurité Cisco du 01 Février 2023:

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-clamav-q8DThCy

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-capic-csrfv-DMx6KSwV
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-lldp-dos-ySCNZOpX
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucsm-bkpsky-H8FCQgsA
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxfp-cmdinj-XXBZjtR
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-elyfex-dos-gfvcByx