Notes de mise à jour pour Cisco Firepower 4100/9300 FXOS version 2.12(1)

Dernière modification : 2024-10-10

Ce document contient des renseignements sur la version Cisco Firepower eXtensible Operating System (FXOS) 2.12.0.

Utilisez ces notes de mise à jour en complément des autres documents énumérés dans la feuille de route de route de documentation :

- http://www.cisco.com/go/firepower9300-docs
- http://www.cisco.com/go/firepower4100-docs

Remarque Les versions en ligne de la documentation utilisateur sont mises à jour occasionnellement après la version initiale. Par conséquent, les renseignements contenus dans la documentation de Cisco.com remplacent tous les renseignements contenus dans l'aide contextuelle qui accompagne le produit.

Introduction

L'appliance de sécurité Cisco est une plateforme de nouvelle génération pour les solutions de sécurité du réseau et du contenu. L'appliance de sécurité fait partie de la solution de sécurité Cisco Application Centric Infrastructure (ACI). Elle fournit une plateforme agile, ouverte et sécurisée, conçue pour l'évolutivité, un contrôle cohérent et une gestion simplifiée.

L'appliance de sécurité offre les fonctionnalités suivantes :

- Système de sécurité modulaire basé sur un châssis – Offre des performances élevées, des configurations d'entrée/sortie flexibles et une grande évolutivité.
- Gestionnaire de châssis –L'interface utilisateur graphique fournit une représentation visuelle rationalisée de l'état actuel du châssis et permet une configuration simplifiée des caractéristiques du châssis.
- CLI FXOS : Fournit une interface basée sur les commandes pour configurer les fonctions, surveiller l'état du châssis et accéder aux fonctions de résolution de problèmes avancées.
- API REST FXOS : Permet aux utilisateurs de configurer et de gérer leur châssis de manière programmatique.

Quoi de neuf

Nouvelles fonctionnalités de FXOS 2.12.1.84

Correction de divers problèmes (voir Bogues résolus dans la version FXOS 2.12.1.84, à la page 20).

Nouvelles fonctionnalités de FXOS 2.12.1.72

Correction de divers problèmes (voir Bogues résolus dans la version FXOS 2.12.1.72, à la page 19).

Nouvelles fonctionnalités de FXOS 2.12.1.48

Correction de divers problèmes (voir Bogues résolus dans la version FXOS 2.12.1.48, à la page 18).

Nouvelles fonctionnalités de FXOS 2.12.1.29

Correction de divers problèmes (voir Bogues résolus dans la version FXOS 2.12.1.29, à la page 16).

Nouvelles fonctionnalités de FXOS 2.12.0.498

Correction de divers problèmes (voir Bogues résolus dans la version FXOS 2.12.0.498, à la page 12).

Nouvelles fonctionnalités de FXOS 2.12.0.467

Correction de divers problèmes (voir Bogues résolus dans la version FXOS 2.12.0.467).

Nouvelles fonctionnalités de FXOS 2.12.0.450

Correction de divers problèmes (voir Bogues résolus dans la version FXOS 2.12.0.450).

Nouvelles fonctionnalités de FXOS 2.12.0.432

Correction de divers problèmes (voir Bogues résolus dans la version FXOS 2.12.0.432).

Nouvelles fonctionnalités de FXOS 2.12.0.31

Correction de divers problèmes (voir Bogues résolus dans la version FXOS 2.12.0.31).

Cisco FXOS 2.12.0 présente les nouvelles fonctionnalités suivantes :

Tableau 1 : Nouvelles fonctionnalités de FXOS 2.12.0

Fonctionnalités	Description
QoS de CLI	Vous pouvez maintenant utiliser l'interface de ligne de commande **show interface ethernet <slot> <port> match statistics** pour suivre les abandons intermédiaires qui se produisent sur la TCAM Vous pouvez maintenant contrôler les files d'attente de trafic à l'aide de l'interface de ligne de commande **show interface ethernet <slot> <port> policer statistics police** pour éviter que les débits de trafic exorbitants ne passent par des files d'attente de priorité stricte Vous pouvez maintenant contrôler les débits de trafic à l'aide de l'interface de ligne de commande **show queuing interface ethernet <slot> <port>** pendant une congestion pour éviter la perte de paquets de données
Chemin des paquets du commutateur	Vous pouvez maintenant déboguer le problème associé au chemin des paquets du commutateur pour les appareils Secure Firewall 3100

Fonctionnalités	Description
Unification des appareils de sécurité adaptables Cisco et de FTD SNMP	Vous pouvez maintenant configurer le menu déroulant **Admin Instance** (instance de l'admin) pour l'unification SNMP des appareils de sécurité adaptables Cisco et de FTD.

Téléchargement de logiciel

Vous pouvez télécharger des images logicielles pour FXOS et les applications prises en charge à partir de l'une des URL suivantes :

- Firepower 9300 — https://software.cisco.com/download/type.html?mdfid=286287252
- Firepower 4100 — https://software.cisco.com/download/navigator.html?mdfid=286305164

Pour en savoir plus sur les applications prises en charge par une version particulière de FXOS, consultez le guide sur la *compatibilité de Cisco FXOS* à cette URL :

https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/compatibility/fxos-compatibility.html

Remarques importantes

- Dans les versions FXOS 2.4(1) ou ultérieures, si vous utilisez un canal IPSec sécurisé en mode FIPS, l'entité homologue IPSec doit prendre en charge le RFC 7427.
- Lorsque vous configurez Radware DefensePro (vDP) dans une chaîne de services sur une Défense contre les menacesapplication en cours d'exécution sur un appareil Firepower 4110 ou 4120, l'installation échoue et envoie une alarme de défaillance. En guise de solution de rechange, arrêtez l'instance de l'application Défense contre les menaces avant d'installer l'application Radware DefensePro.

Remarque Ce problème et la solution de rechange s'appliquent à toutes les versions prises en charge de la chaîne de service Radware DefensePro avec Défense contre les menaces sur les appareils Firepower 4110 et 4120.

- Mise à jour du micrologiciel : nous recommandons que vous mettiez à jour votre appareil de sécurité Firepower 4100/9300 au micrologiciel le plus récent. Pour en savoir plus sur la façon d'installer une mise à jour du micrologiciel et sur les correctifs inclus dans chacune des mises à jour, consultez l'adresse https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/firmware-upgrade/fxos-firmware-upgrade.html.
- Lorsque vous effectuez la mise à niveau d'un module de réseau ou de sécurité, certaines défaillances sont générées, puis éliminées automatiquement. Cela comprend une défaillance indiquant que l'échange à chaud n'est pas pris en charge ou que le module a été supprimé alors qu'il était à l'état en ligne. Si vous avez suivi les procédures appropriées, comme elles sont décrites dans le Guide d'installation du matériel Cisco Firepower 9300 ou le Guide d'installation du matériel de la série Cisco Firepower 4100, les défaillances sont automatiquement éliminées et aucune action supplémentaire n'est requise.

Configuration système requise

- Vous pouvez accéder à gestionnaire de châssis en utilisant les navigateurs suivants :
  - Mozilla Firefox — version 42 et ultérieures

- Google Chrome — version 47 et ultérieures
- Microsoft Internet Explorer – version 11 et ultérieures

Nous avons testé FXOS 2.12.0 avec Mozilla Firefox version 42, Google Chrome version 47 et Internet Explorer version 11. Les autres versions de ces navigateurs devraient fonctionner. Toutefois, si vous éprouvez des problèmes liés à votre navigateur, nous vous suggérons d'utiliser l'une des versions testées.

Directives de mise à niveau

Vous pouvez faire passer vos appareils de sécurité des gammes Firepower 9300 ou Firepower 4100 directement à la version FXOS 2.12.0 s'ils utilisent la version 2.2(2) ou toute version ultérieure. Avant de faire passer vos appareils de sécurité des gammes Firepower 9300 ou Firepower 4100 à la version FXOS 2.12.0, vous devez d'abord effectuer la mise à niveau à la version FXOS 2.2(2) ou vous assurer qu'ils utilisent déjà la version FXOS 2.2(2).

Pour obtenir des directives sur la mise à niveau, consultez le Guide de mise à niveau Cisco Firepower 4100/9300.

Remarques concernant l'installation

- Une mise à niveau à la version FXOS 2.12.0 peut prendre jusqu'à 45 minutes. Planifiez vos activités de mise à niveau en conséquence.
- Si vous mettez à niveau un appareil de sécurité des séries Firepower 9300 ou Firewall 4100 qui utilise un appareil logique autonome ou si vous mettez à niveau un appareil de sécurité Firepower 9300 qui utilise une grappe dans un châssis, le trafic ne passera pas par l'appareil pendant la mise à niveau.
- Si vous mettez à niveau un appareil de sécurité Firepower 9300 ou Firepower 4100 faisant partie d'un regroupement inter-châssis, le trafic ne passe pas par l'appareil mis à niveau pendant la mise à niveau. Cependant, les autres appareils du groupe continuent de laisser le trafic circuler.
- La rétrogradation des images FXOS n'est pas officiellement prise en charge. La seule méthode prise en charge par Cisco pour rétrograder une version d'image FXOS consiste à effectuer une recréation d'image complète de l'appareil.

Bogues résolus et ouverts

Les bogues résolus et ouverts pour cette version sont accessibles dans l'outil de recherche de bogues de Cisco. Cet outil Web vous permet d'accéder au système de suivi des bogues de Cisco, qui conserve les informations sur les bogues et les vulnérabilités de ce produit et d'autres produits matériels et logiciels de Cisco.

Remarque Vous devez avoir un compte Cisco.com pour vous connecter et accéder à l'outil de recherche de bogues de Cisco. Si vous n'en avez pas, vous pouvez accéder au Cisco.com.

Pour plus de renseignements sur l'outil de recherche de bogues de Cisco, consultez l'aide et FAQ de l'outil de recherche de bogues.

Bogues ouverts dans la version FXOS 2.12.0.31

Le tableau suivant répertorie les bogues ouverts dans FXOS, version 2.12.0.31 :

Numéro d'identification de la mise en garde	Description
CSCwc03242	BC01_IBMC01_showTechSupport_log généré lors de la collecte des journaux d'assistance technique

Bogues résolus dans la version FXOS 2.12.0.31

Le tableau suivant répertorie les bogues déjà indiqués dans la version précédente et trouvés par le client, puis résolus dans FXOS 2.12.0.31 :

Numéro d'identification de la mise en garde	Description
CSCvoty83696	Amélioration : Journaux de traitement FPR 4100/9300 bcm_usd pour prendre en charge une éventuelle ACR
CSCwa03285	Mise à niveau vers 2.10.1.666 entraîne la dégradation de SM - format de micrologiciel non reconnu
CSCwa85297	Les VLAN du canal de port internes multi-instances peuvent être mal programmés, ce qui entraîne une perte de trafic
CSCvu36664	État opérationnel de FXOS : Problème thermique par intermittence
CSCvx76651	Amélioration : Empêche l'adressage IP CCL sur le sous-réseau 169.254.xx lors de la création de la grappe
CSCvz01271	Commande show requise pour voir les détails de l'émetteur-récepteur du port de gestion FXOS par l'entremise de l'interface de ligne de commande
CSCvz94217	Version de départ de l'instance d'application est ignorée et définie comme version en cours après copie de la configuration
CSCwa52215	Téléchargement du micrologiciel déclenche l'oscillation du canal de port de données
CSCwb84638	Amélioration du gestionnaire de ports / LACP pour enregistrer les événements de journalisation lors des redémarrages en raison d'événements externes
CSCvz72467	Déni de service pour le protocole de découverte des logiciels Cisco FXOS et NX-OS
CSCwa55772	Rechargement inattendu dans FPR 4100 avec la raison « Reset triggered due to HA policy of Reset »
CSCvu76180	Demande de convivialité – Ajout d'un message d'erreur indiquant que le micrologiciel du FXOS n'est pas entièrement activé
CSCvy83657	Suppression ou élagage du noyau du processus FXOS des fichiers système (aucune validation)
CSCvz14640	Utilisation du répertoire temporaire du système FXOS étonnamment élevée

Numéro d'identification de la mise en garde	Description
CSCvz50201	FXOS peut afficher l'erreur F1256 concernant le disque local 0 manquant
CSCvy48764	Accès avec SSH et authentification par clé publique nécessite un mot de passe utilisateur
CSCvy95497	Mise à niveau du micrologiciel SSD du châssis peut être bloquée de manière incorrecte
CSCvy80380	Augmentation de l'utilisation du disque /var/tmp dans le châssis FPR4150-ASA
CSCvz01285	Commande show requise pour voir les détails de la version de FPGA sur les périphériques Firepower
CSCvz94740	Service de recherche de la source et de rechargement pour FXOS en raison de l'envoi de SIGABRT par le service « ascii-cfg » pour ne pas avoir défini de pulsation.
CSCwb74357	Aucune rotation des fichiers journaux pour la partition opt_cisco_platform_logs dans FXOS
CSCwa62167	CIAM : Apache-http-server CVE-2021-44790 et CVE-2021-44224
CSCvz71282	FXOS | Compteur d'erreurs d'alignement élevé sur le canal de port 48
CSCvz91266	FXOS – Un uri-path de demande spécialement conçu peut pousser mod_proxy à transférer la demande à un serveur d'origine
CSCvt13808	Amélioration : FP 4100/9300 – Unification de FTD et de SNMP dans FXOS
CSCvx04995	Défaillance F0736 ne devrait pas être générée en raison d'une passerelle par défaut inaccessible
CSCvy81369	Amélioration : Inclure la sortie de la commande dmesg -T dans les fichiers d'affichage technique de FXOS
CSCwb15170	Panne en vue du port RM 1120 avec vitesse de 100/10 et conditions de duplex intégral/partiel, vitesse et duplex ne correspondent pas
CSCwb73356	Journaux de nvRAM écrits toutes les deux secondes, ce qui entraîne une utilisation élevée du disque

Bogues résolus dans la version FXOS 2.12.0.432

Le tableau suivant répertorie les bogues déjà indiqués dans la version précédente et trouvés par le client, puis résolus dans FXOS 2.12.0.432 :

Numéro d'identification de la mise en garde	Description
CSCvy99348	Commande Shutdown qui redémarre l'appareil FP1k au lieu de l'éteindre.
CSCwb49416	Recherche de la source du snmpd sur les appareils de sécurité adaptables Cisco et sur les cœurs dans une unité active

Numéro d'identification de la mise en garde	Description
CSCwb90940	Interfaces de données ne s'affichent pas sur l'appareil KP après le déploiement de l'image 9.18.0.14
CSCwc03510	Kilburn Park gèle ou plante lors du chargement du système netboot
CSCwb62059	Connexion impossible à FTD avec l'authentification extérieure après la mise à niveau à niveau de la version 7.0.1---> 7.2.-1947
CSCwb70030	MIO : aucun redémarrage de la lame pendant CATERR si la gravité de la défaillance est non grave ou si le capteur CATERR est différent
CSCwb93924	sFP-detect ne fonctionne pas correctement sur les ports fixes et ePM
CSCwc02133	Injection d'interface Shell racine dans la commande « support fileView » du module de sécurité
CSCwc41590	Échec de mise à niveau et échec de démarrage de l'instance d'application avec l'erreur « CSP_OP_ERROR. CSP signature verification error. » (erreur de vérification de la signature CSP)
CSCvz74356	Interface de gestion des périphériques FDM 1010 n'indique pas le bon état
CSCwa90735	Erreur de rotation des fichiers ASAconsole.log
CSCwa99171	Date du châssis et de l'application revient au 1er janvier 2010 après le redémarrage
CSCwb83756	TPK netmod OIR remplit le journal de messages d'erreur jusqu'à la fin
CSCwc08094	Mettre à jour CiscoSSL à la version 1.1.1o.7.3sp.143
CSCwb58007	FTDv sur Azure – Recherche de la source sur le fil PTHREAD
CSCwa71071	Mise à jour du certificat groupé pour la version 7.2
CSCwb41361	Mise à jour de l'identifiant de validation WR8, LTS18 et LTS21 dans la couche CCM (séq. 26)
CSCwb25246	Fin de la session ASAv SSH avec la commande ospf network avec le concentrateur Azure/ Azure Stack
CSCwc45356	FXOS : prend en charge un seul type de PID pour les plateformes FPR3100
CSCwa88148	Amélioration : Commutation en veille/contournement de la fonction Fail-to-Wire de défaillance au fil à partir de l'interface de ligne de commande
CSCwb10884	WM11xx : Message « ERROR: waiting for fxos_log_shutdown (ERREUR : en attente de FXOS_log_shutdown) » pendant l'arrêt
CSCwb94573	3140 – Défaillance de la plateforme – Code : F1374 - Gravité : Critique

Numéro d'identification de la mise en garde	Description
CSCwb97486	FPR3100 : les ports à fibre optique 25 G peuvent afficher une liaison sur certains ports à fibre optique uniquement compatibles avec le 1/10G
CSCwb27099	FXOS : Interopérabilité tierce entre le serveur Cisco Ciela et un châssis Firepower
CSCwb84638	Amélioration du gestionnaire de ports / LACP pour enregistrer les événements de journalisation lors des redémarrages en raison d'événements externes
CSCwb01633	Journaux absents dans FXOS pour diagnostiquer la cause première de l'échec de la génération du fichier d'affichage technique
CSCwb12465	Autotests FIPS doivent être exécutés lorsque le mode CC est activé - fichiers manquants
CSCwb74357	Aucune rotation des fichiers journaux pour la partition opt_cisco_platform_logs dans FXOS
CSCwb95787	FPR1010 – Aucun ARP sur l'interface VLAN du port du commutateur après l'événement portmanager DIED
CSCwb57988	Recherche de la source dans smConLogger causé par une fuite de mémoire
CSCwb85516	Mettre à jour la mib de l'entité avec les nouveaux détails d'EPM pour WA-B/TPK
CSCwb89065	Avertir lorsque les versions de TPK borough/temple fpga sont inférieures au minimum
CSCwc37196	FPR3100 : Le réseau netmod 8x1G en cuivre peut indiquer par erreur un micrologiciel obsolète au démarrage
CSCwb02689	FXOS devrait vérifier la strate de l'horloge de référence plutôt que la strate de l'horloge locale du serveur NTP
CSCwb40662	Amélioration : Le FCM devrait inclure une option de modification de « link debounce time (délai de l'antirebond du lien) de l'interface
CSCwb46385	Prise en charge de l'API REST pour la configuration du délai de l'antirebond
CSCwb85391	Vérification interrompue de la version de TPK Ctrl-FPGA

Bogues résolus dans la version FXOS 2.12.0.450

Le tableau suivant répertorie les bogues déjà indiqués dans la version précédente et trouvés par le client, puis résolus dans FXOS 2.12.0.450 :

Numéro d'identification de la mise en garde	Description
CSCwb12119	CIAM : expat – CVE-2022-25235 et autres
CSCwb24367	Évaluation du protocole ssp pour la vulnérabilité « Dirty Pipe »

Numéro d'identification de la mise en garde	Description
CSCwb70138	CIAM : python CVE-2015-20107
CSCwc30692	TPK 3140 Maryland : %ERROR% – Switch device not found! during reboot
CSCwb44662	CIAM : zlib - CVE-2018-25032
CSCwb62105	CIAM : glibc 2.33, CVE-2022-23219 et autres
CSCwb71554	CIAM : libxml - CVE-2022-23308
CSCwc30239	CIAM : apache-http-server – CVE-2022-31813 et autres
CSCwc34082	CIAM : curl – CVE-2022-22576 et autres
CSCwc75082	25G-SR devrait prendre la valeur RS-FEC (IEEE CL108) par défaut plutôt que FC-FEC
CSCwb80192	Mise à jour de l'ID de validation WR6, WR8 dans la couche CCM (séq. 30)
CSCwb84967	Fichier de résolution de problèmes pour le châssis de l'appareil Firepower 9300 a causé une panne
CSCwc08676	Mise à jour de l'identifiant de validation WR6, WR8, LTS18 et LTS21 dans la couche CCM (séq. 32)
CSCwc25207	Mise à jour de l'identifiant de validation WR6, WR8, LTS18 et LTS21 dans la couche CCM (séq. 33)
CSCwc46569	Mise à jour de l'identifiant de validation WR8, LTS18 et LTS21 dans la couche CCM (séq. 34)
CSCwc60907	Mise à jour de l'identifiant de validation WR6, WR8, LTS18 et LTS21 dans la couche CCM (séq. 35)
CSCwc69036	Échec, dans TPK 3110, du démarrage à partir de la ligne de référence rommon avec le message « unable to unlock or revert SED »
CSCwc83037	Mise à jour de l'identifiant de validation WR6, WR8, LTS18 et LTS21 dans la couche CCM (séq. 36)
CSCwb71582	CIAM : Strongswan – CVE-2021-45079
CSCwb83166	Mise à niveau vers CiscoSSL FOM 7.3sp et CiscoSSL 1.1.1o.7.3sp.134-fips dans SSP MIO
CSCwc03393	Recherche de la source sur la ligne et taille du fichier principal supérieurs à 40 G avec échec de compression sur Cisco FTD
CSCwc08374	Adresse MAC du NIC de la carte réseau Azure ASA pour Gigeth 0/1 et 0/2 arrête de fonctionner après l'ajout d'interfaces

Numéro d'identification de la mise en garde	Description
CSCwd07413	FMC - Modification des interfaces membres sur le canal de port bloquée dans la fenêtre de mise à jour de l'interface
CSCvz19364	Aucun message syslog envoyé par FXOS quand duplex passe à « Half Duplex »
CSCwb21037	Erreur de licence Smart pour FCM lors de la synchronisation des rapports de licence Smart
CSCwb80108	FP2100/FP1000 : Ports RJ45 intégrés ne s'activent pas de façon aléatoire après les événements de redémarrage du gestionnaire de ports
CSCwb95383	Clé FDM-HA KP à l'état suspendu sans basculement après avoir rétabli la version antérieure, de 7.3 à 7.1
CSCwc25523	Enregistrement de l'appareil pour télémétrie échoue dans les images pour les développeurs en raison des certificats de sécurité manquants
CSCwc31619	TPK : Erreur DME pour ID de carte non valide avec SwitchCardPowerCtrlModule
CSCwc47386	Interface utilisateur Web vFMC inaccessible après l'activation du mode CC dans la version 7.3.0-1553 : ERR_CONNECTION_REFUSED
CSCwc51827	Erreur portmanager Died après l'installation de la version 7.3.x sur wm1010
CSCwc61106	Impossible de configurer le domaine\nom d'utilisateur sous cfg-export-policy dans FXOS
CSCwc75061	FMC permet d'accéder à l'interpréteur de commandes pour le nom d'utilisateur avec « . », mais l'authentification extérieure échouera
CSCwc76195	Interfaces de communication sans fil oscillent par intermittence en raison de l'expiration du délai de surveillance dans la plateforme KP
CSCwd08626	FTW : Paires de ports contournées de façon imprévue en raison d'une défaillance
CSCwd09546	WA : la routine sFP OIR de gestionnaire de ports utilise une table insuffisante pour l'antirebond du module
CSCvz42084	Mise à jour du pilote msmtp pour corriger les échecs de l'envoi de courriels SMTP dans FMC
CSCvz44638	Modifications dans FXOS pour CSCky86319 – Les données ne sont pas détruites après le formatage du disk0 sur ISA3K
CSCwb57524	Échec de la mise à niveau de FTD - Espace disque insuffisant en raison des anciens ensembles FXOS dans la partition distribuable
CSCwb73678	Avertissement de partition /var/tmp remplie sur FXOS
CSCwb88090	FXOS : Après configuration de FXOS, l'importation d'un nouveau canal de port provoque l'oscillation du canal de port existant

Numéro d'identification de la mise en garde	Description
CSCwb94573	3140 – Défaillance de la plateforme – Code : F1374 - Gravité : Critique
CSCwb94980	TPK : Événements d'insertion SFP manquants pour les ports de fibre optique de base, y compris le port de gestion.
CSCwc08683	Voyant DEL de l'interface reste vert et clignote lorsque la fibre optique est débranchée sur le FPR1150
CSCwc29384	KP – Ajout de segments de mémoire DMA au fichier principal généré par livecore
CSCwc37061	SNMP : FMC ne répond pas à l'OID 1.3.6.1.2.1.25.3.3.1.2
CSCwc41591	[IMS_7_3_0] cor.portmgr_ipc trouvé sur WM1010 lors du redéploiement de toutes les politiques
CSCwc46847	Partition FXOS opt_cisco_platform_logs sur FP1K/FPR2K peut être pleine en raison du fichier ucssh_*.log
CSCwc60463	Aucune rotation des fichiers journaux pour la partition opt_cisco_platform_logs dans FXOS
CSCwc94062	[FTDv/Kenton/ISA3k - FXOS] Ajout de la capacité de superviser sshd pour le redémarrer en cas d'échec
CSCwc94670	Fuite de mémoire dans svc_sam_statsAG dans TPK
CSCvz77202	RMU a lu les entrées périmées sur le lien ctrl int entre le processeur x86 de Denverton et le commutateur 88E6390X de Marvel
CSCwb77818	Télémétrie reste à l'état activé même après l'annulation de l'enregistrement de SL de la CLI
CSCwc77879	Prise en charge de l'utilitaire Autopy Uncore pour la succursale du Vermont
CSCwc32584	WM 1150 : Échec de la mise à niveau vers l'image asa « 99.16.4.24-198 » sur la plateforme Wm1150
CSCwb48166	Mise à niveau de FXOS à la version 2.11 est bloquée
CSCwb66175	MIO n'est pas en mesure d'enregistrer le problème de traitement lié au processus appAG
CSCwc76849	Propagation de l'état du lien arrête de fonctionner lors du redémarrage complet du châssis
CSCwc26489	Amélioration – Définition de la politique et de la priorité de planification de zmqio pour le réseau des partenaires de pulsation MIO
CSCwc74905	FXOS : Les ports 7 et 8 de FPR-X-NM-8X10G ne sont pas configurables.

Bogues résolus dans la version FXOS 2.12.0.467

Le tableau suivant répertorie les bogues déjà indiqués dans la version précédente et trouvés par le client, puis résolus dans FXOS 2.12.0.467 :

Numéro d'identification de la mise en garde	Description
CSCwc37695	En plus de l'injection de commande shell c_rehash identifiée dans CVE-2022-1292
CSCwc82169	Découverte de la lame FPR4100/9300 peut se bloquer en raison d'une défaillance de la communication interne avec l'adaptateur de lame
CSCwd31427	FMC autorisant une version en format explicite des paramètres EC avec syslog sur TLS en mode CC
CSCwd34662	Mise à jour de l'identifiant de validation LTS18 et LTS21 dans la couche CCM (séq. 39)
CSCwb89257	Échec de connexion d'un utilisateur distant avec accès SSH et méthode d'authentification par mot de passe après la mise à niveau de FXOS
CSCwc57204	FXOS ne répond pas à la connexion SSH
CSCwc87441	Pour les processus système, limiter les CPU utilisées au nombre de CPU système
CSCwd06758	Aucune validation d'entrée pour les serveurs DNS des appareils logiques dans la configuration de démarrage sur le gestionnaire de châssis
CSCwd37560	Ajout de l'option forceReboot pour l'API REST d'installation groupée
CSCwd45784	Mise à jour du moteur FXOS SWIMS à la version 3.0.4
CSCwd45904	Livecore ne renvoie pas le code erreur approprié lorsqu'il n'y a pas d'espace
CSCwd47340	Fuite de mémoire potentielle dans le processus svc_sam_envAG
CSCwb52656	Journaux de trace SNM avec horodatages incorrects
CSCwd47481	Mise à jour de l'identifiant de validation WR6, WR8, LTS18 et LTS21 dans la couche CCM (séq. 40)
CSCwd65327	Mise à jour de l'identifiant de validation WR6, WR8, LTS18 et LTS21 dans la couche CCM (séq. 41)
CSCwc96726	R2130 utilise le site distant/la succursale du système d'exploitation Wave CIS_LTS21_R2130 pour la version 7.3.0 bêta 2.

Bogues résolus dans la version FXOS 2.12.0.498

Le tableau suivant répertorie les bogues déjà indiqués dans la version précédente et trouvés par le client, puis résolus dans FXOS 2.12.0.498 :

Numéro d'identification de la mise en garde	Description
CSCwe07734	L'appareil de sécurité adaptable Cisco passe en mode de sécurité intégrée après la mise à mise à niveau de FXOS
CSCwb24306	Entrée de journal en double pour /mnt/disk0/log/asa_snmp.log
CSCwc49353	Paire QP MI FTD HA passe à l'état désactivé
CSCwc83495	Ajout de la commande abort dans switch_driver pour faire planter le gestionnaire de ports lorsque les udbs sont corrompus
CSCwd58188	État de la paire en ligne n'a pas pu passer du mode de contournement matériel au mode veille
CSCwd68346	Défaillance de pulsation de la lame MIO de l'appareil de sécurité adaptable Cisco en raison d'un plantage du noyau Linux vers le cœur MEZZ
CSCwd72680	FXOS : temps d'arrêt du FP2100 FTW déclenché par une utilisation élevée du processeur pendant le déploiement de la politique de contrôle d'accès sur Cisco FTD
CSCwd74839	Plus de 30 secondes de perte de données lorsque l'unité rejoint la grappe
CSCwd89349	Mise à jour de l'identifiant de validation WR6, WR8, LTS18 et LTS21 dans la couche CCM (séq. 42)
CSCwd95415	Appareil en veille devient en état de défaillance en raison d'une défaillance du signal de pulsation du renifleur
CSCwd96766	41xx : Lame n'enregistre pas ou ne journalise pas le signal de redémarrage
CSCwd99885	Mauvais changement de code pour portmgr_ipc.c
CSCwe14619	Appareil de secours entre en état de défaillance en raison d'un échec de pulsation du renifleur (Precommit Build Failure)
CSCwe20714	Trafic 7.4.0-1603 WA/TPK-HA ne fonctionne pas pour une interface d'adresse MAC non statique
CSCwe24532	Plusieurs instances des fichiers journaux nvram.out ont fait l'objet d'une rotation sous /opt/cisco/platform/logs/
CSCwe25025	Impossible de mettre en ligne Netmod 8 x 10 Go
CSCwe30653	Échec de la mise à mise à niveau de FTD à « 999_finish/999_zz_install_bundle.sh » en raison d'un mauvais certificat de clé
CSCwe32394	abort/reload ssp : Arrêt appelé après le lancement d'une instance de « Stb::ad_alloc » à partir de la commande surcharge.cpp
CSCwe51412	Canal de port inactif avec état suspendu sur les ports membres

Numéro d'identification de la mise en garde	Description
CSCvx71936	FXOS : Défaillance « The password encryption key has not been set. » affichée sur les appareils FPR1000 et FPR2100
CSCwa75392	Message d'avertissement manquant lors de la mise à niveau de FXOS
CSCwb30042	SA pour msglyr et le code switch/src/HAL_Layer code
CSCwc10545	system_pid_specific_misc_defs.json a des cœurs système incorrects pour TPK
CSCwc12719	Modifier le fichier d'assistance technique pour saisir d'autres informations de débogage (commande show portmanager switch vlans)
CSCwc34801	[IMS_7_3_0]REST_API : Network::getMTU [ERROR] au moment de définir les informations sur le réseau lors du premier démarrage
CSCwc69977	Vérification du pointeur nul manquant dans la routine d'affichage sfp
CSCwc83851	Erreurs OIR dans portmgr.out
CSCwd10139	Commande ping vers ipv6 gw entraîne une panne du système, fonctionne sans lui
CSCwd12978	WA-B : Commande show env pour les appareils de sécurité adaptables Cisco affiche incorrectement les informations sur le bloc d'alimentation
CSCwd43666	Analyse de la raison pour laquelle il n'y a pas de logrotate pour /opt/cisco/config/var/log/ASAconsole.log
CSCwd53448	FPR3100 : Voyants DEL du module de réseau 4 x 40 ne clignotent pas lorsqu'il y a du trafic
CSCwd56266	KP-FTP sous local-mgmt ne fonctionne pas
CSCwd56462	LLDP : Voisins non détectés sur le premier port de déploiement sans suppression de la configuration lldp
CSCwd68159	LLDP : Suppression d'un port membre du canal de port supprime complètement les voisins lldp
CSCwd82787	Erreurs de demande de mise à niveau inondent portmgr.out après le retrait de netmod
CSCwd92804	Voyant DEL du ventilateur clignote en ambre sur FPR2100
CSCwd95063	npu accel - nam_client ipc_recv_timeouts - touche les appels de statistiques npu-accel local-mgmt, lina de FXOS
CSCwe02421	FPR-X-NM-6X1SX-F non reconnu sur FP3100 ou FP4200
CSCwe13577	Journal d'audit manquant pour la modification du port de gestion
CSCwe18145	Vtesse d'interface n'est pas mise à jour sur Cisco FTD

Numéro d'identification de la mise en garde	Description
CSCwe21569	Amélioration des options de l'interface de ligne de commande la gestion de l'IP avec l'option DHCP
CSCwe22302	Partition « /opt/cisco/config » est pleine en raison d'une rotation insuffisante du journal du fichier wtmp
CSCwe32972	stdout_env_manager.log est rempli de messages de tableau de type 3 inconnus
CSCwe33910	sr_build.log comprend les trois mêmes messages répétés toutes les minutes
CSCwe33943	svc_sam_serviceOrchAG.log est rempli de messages sans valeur qui se répètent chaque minute
CSCwe36758	3105 : F78672 après un redémarrage
CSCwe48918	LTS18 CCM numéro de séquence 44 pour mettre à mettre à jour la libjitterentropy à la version 3.4.1
CSCwe59989	Solution de contournement pour corriger la défaillance de la version introduite par la validation CCM de Wind River
CSCwe63794	Réduction du niveau de gravité des défaillances pour la dégradation RAID en raison d'un disque toujours en état de rechange
CSCwb88729	FTD – %FTD-3-99015 : port-manager : erreur : échec de lecture du bloc DOC, port X, st = X log
CSCwe24440	Description de suppression du contrôleur de disque remove/remove-secure ne correspond pas
CSCwe34512	JENT : Ajout de la bibliothèque JENT à fxos pour prendre en charge KP
CSCwd35074	Échec d'enregistrement de la télémétrie dans la version 2.13
CSCwd99813	Superviseur ne redémarre pas le module ou la lame qui ne répond pas en raison d'un problème CATERR avec un ID de capteur de gravité mineur 50
CSCwe33130	Superviseur ne redémarre pas le module ou la lame qui ne répond pas en raison d'un problème IERR avec un ID de capteur de gravité mineur 79
CSCvx62999	Rejets d'entrée non nuls dans l'interface MI CCL
CSCwb40008	Parfois, le périphérique doit redémarrer lors de la mise sous tension d'alperton netmod dans le périphérique 4100
CSCwb80881	Noyau CSSMGR_log trouvé lors du test de déroutement SNMP sur la version 2.8.1.184
CSCwc79216	Mise à jour du correctif de la trousse de développement de logiciels (SDK) de Broadcom pour la notification d'alerte sur le terrain pour Trident2
CSCwe22152	Cœurs SNMPD vus dans in snmp_sess_Close et notifyTable_register_notifications

Numéro d'identification de la mise en garde	Description
CSCwe19968	Amélioration permettant de journaliser le retard de lancement de FTW et de compenser le retard de lancement
CSCwe59809	Mise à jour de l'ID de validation WR6, WR8, LTS18 et LTS21 dans la couche CCM (séq. 45)
CSCwc49180	Réinitialisation de Statsclient hap et boucle de démarrage de SNMP après l'activation de l'unification de SNMP dans 92.13

Bogues résolus dans la version FXOS 2.12.1.29

Le tableau suivant répertorie les bogues déjà indiqués dans la version précédente et trouvés par le client, puis résolus dans FXOS 2.12.1.29 :

Identifiant	En-tête :
CSCwb75786	Échec de déploiement vu comme « argument content is null » (contenu de l'argument est nul) dans la solution 730
CSCwd34288	FP1000 - Pendant le processus de démarrage en mode LINA, il y a eu des fuites de diffusions entre les interfaces, ce qui a provoqué une tempête
CSCwd94183	Non affichage de la lame après la mise à jour de FXOS pour instances multiples en raison d'un problème de rotation du journal ssp_ntp.log
CSCwe30867	Solution de contournement pour définir hwclock à partir des journaux de ntp sur les plates-formes bas de gamme
CSCwe74916	Interface HORS SERVICE dans un ensemble en ligne avec état propagate pour le lien
CSCwe88600	Plantage silencieux de vFTD sshd, probablement dû aux sondes avec LB dans Azure
CSCwe93802	Mise à jour de l'identifiant de validation WR6, LTS18 et LTS21 dans la couche CCM (séq. 46)
CSCwf08515	FPR3100 : Impact élevé du trafic des appareils de sécurité adaptables Cisco/Cisco FTD sur toutes les interfaces de données avec un nombre élevé de « demux drops »
CSCwf014729	Nécessité d'utiliser CiscoSSL avec FOM 7.3 pour les versions d'Intel
CSCwf17858	Noeud quitte la grappe TPK en raison d'un échec du contrôle d'intégrité de l'interface
CSCwc76419	Journaux d'erreur inutiles du ventilateur doivent être supprimés du fichier thermique
CSCwd67101	FPR1150 : Erreur de format d'exécution constatée et appareil bloqué jusqu'au rechargement, après exécution de « secure all »
CSCwd81123	Utilisation élevée du processeur sur FXOS pour les processus smConlogging
CSCwe50993	SNMP sur le module SFR s'éteint et ne se rallume pas

Identifiant	En-tête :
CSCwe70472	Mise à niveau du composant tiers rng-tools à la dernière version 6.16
CSCwe90524	Amélioration : Ajout d'un horodatage dans le message IPC de l'interface
CSCwf03490	portmanager.sh affiche les avertissements bash continus dans les fichiers journaux
CSCwf16278	Port TPK 2.12 MGMT n'est pas en mesure d'envoyer un message Ping à la passerelle après l'installation de l'application
CSCwf22483	SSH vers châssis permet une prise de contact tridirectionnelle pour les adresses IP qui ne sont pas autorisées par la configuration
CSCwf37871	Tentative de passer à la version 1.19.4 dans les succursales LTS18, mais retour à la version 1.12.12.
CSCwf40113	TPK/WA - Paquets OSPF atterrissent dans plusieurs anneaux RX
CSCwf18647	Modification des paramètres de squelch de Brentwood et de Maryland manquante dans les variantes _X netmod
CSCvz91293	Amélioration : Inclure la configuration de châssis exportée dans le fichier d'affichage technique du châssis pour les techniciens
CSCwc12716	Modification de l'assistance technique pour obtenir des informations de débogage supplémentaires (détails du registre de liaison de contrôle)
CSCwd34920	Amélioration : Besoin de préserver topout.log pour que les données d'au moins les cinq derniers jours soient conservés
CSCwe45653	Amélioration : FXOS doit effectuer le suivre du problème lié au dépassement du quota de disque du module Security
CSCwe79517	Amélioration : TPK affiche les compteurs du gestionnaire de ports pour vidanger les compteurs des règles de rejet par défaut
CSCwe64773	Fichier core.svc_sam_dcosAG observé sur l'appareil après l'effacement de la configuration
CSCwe83544	Après la mise à niveau, l'interface ha reste bloquée sur un nœud
CSCwa98094	Il manque des renseignements sur le MI dans l'assistance technique
CSCwf16886	Les p4tickets universels sont en texte brut dans le code source
CSCvz69950	Inclure la sortie de la commande « show storage detail » dans le fichier FPR3100 FPRM/tech_support_brief
CSCwb06934	Inclure la sortie de la commande « show slot expand detail » dans le fichier tech_support_brief du FPR3100

Bogues résolus dans la version FXOS 2.12.1.48

Le tableau suivant répertorie les bogues déjà indiqués dans la version précédente et trouvés par le client, puis résolus dans FXOS 2.12.1.48 :

Numéro d'identification de la mise en garde	Description
CSCwe87745	Interface de ligne de commande de FXOS affiche les derniers changements à la programmation
CSCwf57856	Recherche de la source et rechargement de FXOS en raison d'une fuite dans la file d'attente de la mémoire tampon MTS
CSCwh22888	FXOS : Suppression de l'application de l'état dégradé des lames après plusieurs erreurs corrigibles de DIMM
CSCwb71519	Amélioration : F1661 - plus de détails sur le motif de l'échec et l'emplacement du journal
CSCwh82859	Cœurs SSHd trouvés après le test de performances du VPN Azure
CSCvx44261	SNMPv3 : Caractères spéciaux utilisés dans la configuration SNMPv3 de FXOS provoquent des erreurs d'authentification
CSCwf82279	Journalisation excessive des messages ssp-multi-instance-mode dans /opt/cisco/platform/logs/messages
CSCwa65801	Journaux « show ntp all » ne sont pas assez clairs et entraînent incertitude et confusion
CSCwh04730	Plantage des segments de vérification des appareils de sécurité adaptables Cisco/FTD HA lorsque les tampons de mémoire sont corrompus
CSCwe81841	FXOS doit fournir une commande qui affichera le nombre d'heures de puissance totale du châssis/de la lame
CSCwf36066	WM/TPK/WA « FTD only » : Pertes de paquets observées après le retrait du membre du PC du canal de port
CSCwh54477	Affichage par le FMC dMune alerte « The password encryption key has not been set » pour les périphériques Firepower 1100/2100 et Secure Firewall 3100
CSCwh55178	FXOS : Processus svc_sam_dcosAG plante sans arrêt sur FirePower 4100
CSCwc48701	Cisco Secure Firewall 3100 MI : Instance du ftd ne parvient pas à se mettre en ligne après le redémarrage du châssis
CSCwf95288	Firepower 1000 Switchport transmet le trafic CDP
CSCwh17366	Mise à jour vers CiscoSSH 1.12.39 dans FXOS
CSCwh18967	Inclusion de « show env tech » dans le dépannage de FXOS FPRM
CSCwh24321	FXOS : Alperton 100G NetMod n'est pas reconnu correctement

Numéro d'identification de la mise en garde	Description
CSCwf44354	JENT : Extension de prise en charge de la bibliothèque JENT à CiscoSSL pour toutes les cibles FXOS
CSCwf55654	Cisco Secure Firewall 3100/4200 – État d'interface incorrect « Management1/1 » sur LINA et FTD
CSCwf63589	Recherche de la source et redémarrage pour le processus snmpd sur Cisco FTD
CSCwh09113	FPR1010 en haute disponibilité n'a pas pu envoyer de données à GARP/ARP ou en recevoir, erreur « \edsa_rcv: out_drop\ »
CSCwb97626	FXOS devrait afficher les journaux ROMMON
CSCwf35500	FXOS/SSP : Système devrait offrir une meilleure visibilité des événements erreur corrigibles de DIMM
CSCwf88124	Ports de commutation en mode Trunk ne transmettent pas le trafic vlan après une perte de courant
CSCwh02371	CCM ID 53 - WR8, LTS18, LTS21

Bogues résolus dans la version FXOS 2.12.1.72

Le tableau suivant répertorie les bogues déjà indiqués dans la version précédente et trouvés par le client, puis résolus dans FXOS 2.12.1.72 :

Numéro d'identification de la mise en garde	Description
CSCvx69675	Défaillances majeures de FXOS concernant la panne de l'hôte de l'adaptateur et de l'interface virtuelle.
CSCwf99303	Interface utilisateur de gestion qui présente un certificat autosigné plutôt qu'un certificat personnalisé signé par l'Autorité de certification (CA) après la mise à niveau.
CSCwi60249	Serveur de secours WM1010E qui ne parvient pas à rejoindre la haute disponibilité avec le message « CD App Sync error is SSP Config Generation Failure » (erreur de synchronisation de l'application de CD correspond à un échec de génération de configuration du SSP).
CSCwi22296	Application logique qui déclenchera un démarrage en mode de sécurité intégrée en raison de la trop grande taille de la configuration.
CSCwi13134	Contournement matériel ne fonctionne pas comme prévu dans FP3140.
CSCwi34600	Connexion par clé du protocole SSH ne fonctionne pas dans ASAv dans lequel la configuration par défaut sur GCP est chargée.
CSCwi62683	Mise à niveau à CiscoSSH 1.13.46 dans FXOS à l'adresse CVE-2023-48795.

Numéro d'identification de la mise en garde	Description
CSCwi10927	TPK/kp/WM : impossible de copier les fichiers techsupport/ts/core sur le serveur.
CSCwf11877	TPK 3110 – INCOMPATIBILITÉ de la version du micrologiciel après la mise à niveau à la version 7.2.4-144.
CSCwe93736	Appareil de sécurité adaptable Cisco ne met pas à jour le fuseau horaire malgré les commandes.
CSCwi80465	CCM ID 63 - LTS18
CSCwh53276	Mise à niveau à CiscoSSL 1.1.1v.7.3.338-fips dans SSP MIO.
CSCwi90399	Horloge du système de Cisco FTD ou des appareils de sécurité adaptables Cisco réinitialisée à 2023.
CSCwf62228	Fuseau horaire ne fonctionne pas correctement sur les plateformes 9300/4100

Bogues résolus dans la version FXOS 2.12.1.84

Le tableau suivant répertorie les bogues déjà indiqués dans la version précédente et trouvés par le client, puis résolus dans FXOS 2.12.1.84 :

Identifiant	En-tête :
CSCwj14927	Cisco FTD : le serveur principal joue un rôle actif après le rechargement
CSCwe82107	Alerte d'intégrité pour [FSM:STAGE:FAILED] : configuration du serveur avec protocole AAA (authentication, authorization and accounting) externe
CSCwi60430	CVE-2023-51385 (niveau de gravité moyen) Dans SSH dans OpenSSH utilisant la version précédente à 9.6, l'injection de commande de système d'exploitation peut se produire si un
CSCwk64418	Protocole NTP ne se synchronise pas lors de l'utilisation de l'authentification SHA-1
CSCwi24007	Problème découvert dans le noyau Linux des versions antérieures à 6.3.3. Il existe un
CSCwi84615	Certains journaux stdout non soumis à la rotation par logrotate
CSCwi56743	Paramètre de quota MSP incorrect pour les instances
CSCwi24116	Twisted est un cadre basé sur les événements pour les applications Internet Antérieur à
CSCwb02701	FXOS ne relance pas la synchronisation NTP avec les serveurs
CSCvx74133	Instance d'application s'affiche comme démarrée au lieu d'en ligne
CSCwk44245	Vulnérabilité suivante résolue dans le noyau Linux : i
CSCwk44246	Vulnérabilité suivante résolue dans le noyau Linux : i

Identifiant	En-tête :
CSCwi78370	41xx/93xx : mise à jour CiscoSSH (gestionnaire de châssis FXOS) pour l'adresse CVE-2023-48795
CSCwi80465	CCM ID 63 - LTS18
CSCvz59859	Description de la défaillance F1758 ne doit pas être spécifiques aux sous-interfaces
CSCwj89050	Validation d'entrée défectueuse dans Apache permet aux attaques ou
CSCwj89051	Dans GNU tar avant la version 1.35, attributs d'extension mal gérés dans une archive PAX
CSCwj89054	Agresseur qui peut forcer un terminal HTTP/2 à lire des quantités quelconques de
CSCwi75967	CCM ID 62 - LTS18
CSCwj43466	Vulnérabilité de débordement de la mémoire tampon trouvée dans LibTIFF, dans extractI
CSCwj08023	Certains aspects DNSSEC du protocole DNS (dans RFC 4033, 4034, 4035, 6
CSCwj08021	Code d'analyse du message DNS dans « named » comprend une section dont
CSCwk59458	21xx : blocages du processus de débogage qui empêchent la récupération des opérations d'écriture bloquées
CSCwj89404	Vulnérabilité suivante résolue dans le noyau Linux : b
CSCwk57933	Vulnérabilités dans le noyau Linux CVE-2023-52439
CSCwj89402	Vulnérabilité suivante résolue dans le noyau Linux : n
CSCwh94193	urllib3 est une bibliothèque cliente HTTP conviviale pour Python. urllib3 doe
CSCwi78191	Problème découvert dans drivers/input/input.c dans le noyau Linux b
CSCwi78193	Problème découvert dans le noyau Linux des versions antérieures à 6.6.8. do_vcc_ioctl
CSCwj89447	inférieur à 653 permet d'exécuter des commandes de système d'exploitation avec un caractère de retour à la ligne i
CSCwj89445	La fonction iconv () de la bibliothèque C GNU versions 2.39 et antérieures peut
CSCwf64429	Impossible de charger l'image de la version FTD dans le FCM
CSCwk64709	Échec de mise à mise à niveau de FXOS en raison d'un manque d'espace disponible dans /mnt/pss (isan.log consomme la majeure partie de l'espace)
CSCwi01323	Protocoles SNMP OID ifOutDiscards sur MIO ont toujours une valeur nulle alors que l'affichage de l'interface d'affichage a une valeur autre que zéro
CSCwj09999	Modification l'unité de transfert maximale du FP 3100 sur interface de gestion ne persiste PAS pendant les redémarrages (le retour à l'unité de transfert par défaut)

Identifiant	En-tête :
CSCwh48776	Problème découvert dans Python avant la version 3.8.18, 3.9.x avant la version 3.9.18,
CSCwk57949	Vulnérabilités dans le noyau Linux CVE-2023-52435
CSCwi36244	Dans versions BuC Traceroute 2.0.12 à 2.1.2 avant 2.1.3, le certificat d'encapsulation
CSCwi92932	copy_params dans rivers/md/dm-ioctl.c dans le noyau Linux jusqu'à la version 6.7.1
CSCwi92930	linux-pam (alias Linux PAM) avant la version 1.6.0 permet aux agresseurs de créer un
CSCwk25759	Vulnérabilité suivante résolue dans le noyau Linux : B
CSCwk25756	Requests est une bibliothèque HTTP. Avant la version 2.32.0, lorsque des demandes sont effectuées au moyen de
CSCwj89434	mur dans util-linux jusqu'à la version 2.40, souvent installée avec setgid tty permi
CSCwk25755	Vulnérabilité suivante résolue dans le noyau Linux : n
CSCwj43355	Bogue dans QEMU pouvant entraîner une opération I/O pour invité autrement adressée à
CSCwe21884	Rédaction d'enveloppe autour de la commande « kill » pour journaliser qui l'appelle
CSCwi85951	Faille de sortie d'urgence trouvée dans __ext4_remount dans fs/ext4/super
CSCwi85953	Dans rds_recv_track_latency dans net/rds/af_rds.c dans le noyau Linux
CSCwj69632	SHA1 est l'algorithme de hachage par défaut pour le certificat du Firepower Chassis Manager sur 4110
CSCwj12924	Faille trouvée dans le sous-système Netfilter, dans le noyau Linux Le i
CSCwk62296	Vulnérabilité dans l'adresse SSP OpenSSH regreSSHion
CSCwi92924	Problème de fuite de mémoire trouvé dans ctnetlien_creer_connTrack dans net/n
CSCwi92927	Vulnérabilité de cycle d'utilisation après interruption de service dans le netfilter, dans le noyau Linux : nf_table
CSCwi36311	Utilise la fonction d'arrêt (kill Tree) dans SMA au lieu de SIGTERM
CSCwj89425	Vulnérabilité suivante résolue dans le noyau Linux : B
CSCwh19613	Appareils de sécurité adapatables Cisco ont planté avec scénarios Saml
CSCwk75035	Vulnérabilité dans le cœur du serveur HTTP Apache 2.4.59 et versions antérieures sont
CSCwk75033	Dans versions antérieures à version 1.21.3 de MIT Kerberos 5 (krb5), un agresseur peut provoquer une commande non va
CSCwh81366	Deuxième disque dur [Multi-Instance] (FPR-MSP-SSD) non utilisé

Identifiant	En-tête :
CSCwh43230	Licence de cryptage renforcé non appliquée aux pare-feux des appareils de sécurité adaptables Cisco dans HA
CSCwh94029	Faille trouvée dans le sous-système Netfilter, dans le noyau Linux Le n
CSCwj08153	Faille de mémoire saturée trouvée dans libtiff qui pourrait être déclenchée par
CSCwk14685	Cisco FTD : Interface de gestion ne fonctionne pas, bien qu'elle soit opérationnelle
CSCwk62297	Évaluation du protocole ssp pour la vulnérabilité regreSSHion dans OpenSSH
CSCwh27886	Gestionnaire de châssis affiche l'erreur du serveur interne HTTP 500 dans des cas spécifiques
CSCwj89417	Vulnérabilité suivante résolue dans le noyau Linux : d
CSCwb02741	État de synchronisation de l'heure et message erreur ne donnent aucun cétail sur le rejet du serveur NTP
CSCwi79120	Certaines sessions SSH n'expirent pas, ce qui empêche ssh et la console de se connecter à la CLI de FXOS
CSCwk50044	Aucune des méthodes Is (IsPrivate, IsLoopback, etc.) indiquées ne fonctionne normalement
CSCwj08083	Problème découvert dans libxml2 versions précédant 2.11.7 et 2.12.x, version précédant 2.1
CSCwj89315	Fractionnement de la réponse HTTP en plusieurs modules dans l'allocation du serveur HTTP Apache
CSCwj08066	Déni de service vulnérabilité en raison d'un blocage trouvé dans sctp_
CSCwj38928	Latence élevée observée sur FPR3120
CSCwf99434	Échec de transfert du nouveau fichier image vers FPR2130 et recherche de la source observée
CSCwk22993	Vulnérabilité suivante résolue dans le noyau Linux : t
CSCwf27337	KP : nettoyage/reformatage du deuxième disque (MSP) lors de la réinstallation de Cisco FTD
CSCwj89406	Vulnérabilité suivante résolue dans le noyau Linux : b
CSCwk25764	Vulnérabilité suivante résolue dans le noyau Linux : H
CSCwk25762	Vulnérabilité suivante résolue dans le noyau Linux : i
CSCwk25761	Vulnérabilité suivante résolue dans le noyau Linux : b
CSCwi78206	Vulnérabilité trouvée dans GnuTLS, où un poste de commande (qui utilise gnuTL
CSCwi78200	Vulnérabilité trouvée dans GnuTLS. Les temps de réponse aux fichiers c malformés

Identifiant	En-tête :
CSCwk75036	Déréférencement du pointeur nul dans mod_proxy du serveur HTTP Apache 2.4.59 et
CSCwk50055	url.c dans GNU Wget jusqu'à 1.24.5 traite mal les points-virgules dans les informations utilisateur
CSCwi04351	Échec de mise à mise à niveau de FTD dans script 999_finish/999_zz_install_bundle.sh
CSCwk75030	Implémentation d'IPv6 dans le noyau Linux jusqu'à version 6.3 a un protocole net/ipv6/
CSCwk05828	nscd : cache du groupe réseau peut mettre fin au démon en cas d'échec d'allocation de mémoire
CSCwk05826	nscd : débordement du tampon basé sur la pile dans le cache du groupe réseau si le nom
CSCwi59271	Suppression du journal système « End of script output before headers » (fin de la sortie du script avant les en-têtes) dans FXOS
CSCwj49958	Échec de négociation du cryptage IPSEC à « Failed to compute a hash value » (échec du calcul de la valeur de hachage)
CSCwi31480	Alerte : échec de désactivation, raison : l'erreur interne n'est pas effacée du FCM ou de l'interface de ligne de commande après l'accusé de réception
CSCwk84221	FPR3100 : interfaces SFP 25G ne se déclenchent pas après le redémarrage
CSCwh94116	Faille trouvée dans le sous-système Netfilter, dans le noyau Linux Le x
CSCwi23964	Python 3.x à 3.10 présente une vulnérabilité de redirection ouverte dans lib/h
CSCwh71262	Faille trouvée dans glibc. Dans une situation peu courante, la commande gaih_inet
CSCwi53987	Paramètres du protocole SSL ne modifient pas la configuration du certificat de l'interface graphique FDM et ne désactivent pas TLSv1.1
CSCwj14028	CCM ID 67 - LTS18
CSCwi00713	Défaut de fuite de mémoire trouvé dans l'utilitaire tiffcrop de Libtiff. Ce problème

Documentation associée

Pour en savoir plus sur l'appareil de sécurité Firepower des gammes 9300 ou 4100 et FXOS, consultez l'orientation dans la documentation sur Cisco FXOS.

Ressources en ligne

Cisco fournit des ressources en ligne pour télécharger de la documentation, des logiciels et des outils, pour rechercher des bogues et pour ouvrir des demandes de service. Utilisez ces ressources pour installer et configurer le logiciel FXOS, ainsi que pour effectuer le dépannage des problèmes techniques et les résoudre.

- Site de soutien et de téléchargement Cisco : https://www.cisco.com/c/en/us/support/index.html

- Outil de recherche de bogues de Cisco : https://tools.cisco.com/bugsearch/
- Service de notification de Cisco : https://www.cisco.com/cisco/support/notifications.html

Vous devez posséder un identifiant utilisateur et un mot de passe sur Cisco.com pour pouvoir accéder à la plupart des outils du site Web d'assistance technique et de téléchargement de Cisco.

Communiquez avec Cisco

Si vous ne pouvez pas résoudre un problème à l'aide des ressources en ligne répertoriées ci-dessus, communiquez avec le centre d'assistance technique Cisco :

- Envoyez un courriel au centre d'assistance technique Cisco : tac@cisco.com
- Appelez le centre d'assistance technique Cisco (Amérique du Nord) : 1.408.526.7209 ou 1.800.553.2447
- Appelez le centre d'assistance technique Cisco (monde entier) : Contacts d'assistance Cisco dans le monde

Communications, services et renseignements supplémentaires

- Pour recevoir des informations pertinentes et opportunes de la part de Cisco, inscrivez-vous sur le gestionnaire de profil Cisco.
- Pour obtenir l'impact commercial que vous recherchez avec les technologies qui comptent, visitez services de Cisco.
- Pour soumettre une demande de service, consultez le service d'assistance de Cisco.
- Pour découvrir et parcourir des applications, des produits, des solutions et des services d'entreprise sécurisés et validés, visitez Cisco MarketPlace.
- Pour obtenir des documents généraux sur la réseautique, la formation et la certification, consultez Cisco Press.
- Pour trouver des informations sur la garantie d'un produit ou d'une famille de produits particuliers, accédez à Cisco Warranty Finder.

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.