Notes de mise à jour pour Cisco Firepower 4100/9300 FXOS version 2.13

Dernière modification : 2024-10-10

Ce document contient des renseignements sur la version Cisco Firepower eXtensible Operating System (FXOS) 2.13.0.

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.
- Cisco Firepower Chassis Manager –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 2.13.0.272

Correction de divers problèmes (voir Bogues résolus dans Bogues résolus dans la version FXOS 2.13.0.272, à la page 5)

Nouvelles fonctionnalités de FXOS 2.13.0.243

Correction de divers problèmes (voir Bogues résolus dans Bogues résolus dans la version FXOS 2.13.0.243, à la page 8)

Nouvelles fonctionnalités de FXOS 2.13.0.212

Correction de divers problèmes (voir Bogues résolus dans la version Bogues résolus dans la version FXOS 2.13.0.212)

Cisco FXOS 2.13.0 présente les nouvelles fonctionnalités suivantes :

Fonctionnalités	Description
Certification avec logo prête pour l'IPv6	Les interfaces de ligne de commande suivantes sont ajoutées pour définir certaines variables sysctl.conf qui persistent après un redémarrage : • set ipv6 enable/disable • set nd enable/disable • set ipv6-auto eui64 • set ipv6-auto stablesec • configuration prête pour l'ipv6 avec adresse ipv6 <var> ipv6-readyconfig eui64 ipv6-readyprefix <var> • set ipv6-ready ipv6-addr <var> ipv6-readyconfig stablesec ipv6-readyprefix <var> La sortie de **show ipv6-if** est mise à jour de manière à afficher les champs suivants : • Autocfg-method • Readycfg-method • État IPv6 • État ND
Détection de fuite de mémoire dans MIO	Vous pouvez maintenant déboguer la fuite de mémoire de chacun des processus à l'aide de la commande mem-leak-logging
Détection de fuites de mémoire dans Cisco Secure Firewall 3100	Vous pouvez maintenant déboguer le processus de fuite de mémoire en activant la fonctionnalité mem-leak-feature

Fonctionnalités	Description
Image unique pour Cisco Secure Firewall 3100	Pour faire passer votre appareil Cisco Secure Firewall 3100 à la version Cisco FTD 7.3.0, vous devez avoir la version 1.1.08 ou ultérieure de ROMMON. Si la version actuelle de ROMMON est antérieure à la version 1.1.08, vous devez mettre à niveau ROMMON en passant à la version 9.19 ou à une version ultérieure de vos appareils de sécurité adaptables Cisco. Vous pouvez également utiliser FMC ou FDM pour faire passer Cisco FTD à la version 7.3.0.
Configuration de Cisco FTD à l'aide de CDO	Vous pouvez maintenant configurer l'appareil FTD à l'aide de CDO.

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 Cisco Firepower Threat Defenseapplication 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 Cisco Firepower Threat Defense 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 Cisco Firepower Threat Defense 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 l'installation d'une mise à mettre à jour de micrologiciel et les correctifs inclus dans chaque mise à mettre 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.

- À compter de la version 2.13, les plateformes suivantes ne sont pas prises en charge :
  - Module de sécurité Firepower 9300 SM-24
  - Module de sécurité Firepower 9300 SM-36
  - Module de sécurité Firepower 9300 SM-44
  - Firepower 4110
  - Firepower 4120
  - Firepower 4140
  - Firepower 4150

Remarque Vous recevrez une erreur lors de l'installation ou de l'exécution des instances de défense contre les menaces sur ces plateformes si elles exécutent FXOS 2.13. Nous vous recommandons d'utiliser la version de FXOS prise en charge ou de changer de matériel. Pour en savoir plus sur les versions de FXOS et le matériel pris en charge, consultez le document Compatibilité de Cisco Firepower 4100/9300.

- À compter de la version FXOS 2.13, la commande **set maxfailedlogins** ne fonctionnera plus. La valeur pourra toujours être définie, mais si vous essayez de vous se connecter avec un mot de mot de passe non valide un nombre de fois supérieur à la valeur déjà définie, votre accès ne sera pas verrouillé À des fins de compatibilité, une commande similaire, soit **set max-login-atempts**, est disponible dans le champ d'application de la sécurité. Cette commande empêche également la connexion après un certain nombre de tentatives infructueuses, mais définit la valeur pour tous les utilisateurs. Ces commandes sont uniquement disponibles pour le mode de plateforme Firepower 2100 et n'affectent aucune autre plateforme.

Configuration système requise

- Vous pouvez accéder à Cisco Firepower Chassis Manager 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 2.13.0 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 2.13.0 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 2.13.0, 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 2.13.0 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 dans la version 2.13.0

Les bogues résolus 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 créer un compte.

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 résolus dans la version FXOS 2.13.0.272

Le tableau suivant répertorie les bogues déjà indiqués dans la version précédente et trouvés par le client, puis résolus dans FXOS 2.13.0.272 :

Identifiant	En-tête :
CSCwh78361	KP/WM : Réception de « \RotatingLogProvider: Internal Error:\ » après la connexion au périphérique
CSCwb84967	FPR4K/FPR9K : Génération d'affichage technique pour le châssis FXOS peut entraîner l'oscillation du port Netmod 40 Go
CSCwc82169	FPR4100/9300 : Trafic élevé redirigé vers le processeur, ce qui entraîne une défaillance de la communication interne avec l'adaptateur de la lame

Identifiant	En-tête :
CSCwd35074	Échec d'enregistrement de la télémétrie dans la version 2.13
CSCwe89256	Firepower Chassis Manager non accessible avec les certificats ECDSA
CSCwf43324	WM1010 : Commande « \Show techsupport fprm brief\ » prend plus de temps que prévu (environ 15 minutes)
CSCwf57856	Recherche de la source FXOS et rechargement causés par une fuite dans la file d'attente de la mémoire tampon MTS
CSCwf88124	Ports de commutation en mode Trunk ne transmettent pas le trafic vlan après une perte de courant
CSCwh01521	Suppression de iotop.cfg de meta-local-dev linux-yocto.bbappend
CSCwh02371	CCM ID 53 - WR8, LTS18, LTS21
CSCwh09113	FPR1010 en haute disponibilité n'a pas pu envoyer de données à GARP/ARP ou en recevoir, erreur « \edsa_rcv: out_drop\ »
CSCwh25636	Problèmes d'apprentissage ARP avec plusieurs instances exécutant Netmod 100G
CSCwh17366	Mise à jour vers CiscoSSH 1.12.39 dans FXOS
CSCwh19613	Appareils de sécurité adapatables Cisco ont planté avec scénarios Saml
CSCwh22916	ID CCM 54 – Mise à jour de WR8, LTS18, LTS21 – (PANNE de LTS21 alors que WR8 et LTS18 fonctionnent)
CSCwh43230	Licence de cryptage renforcé non appliquée aux pare-feux des appareils de sécurité adaptables Cisco dans HA
CSCwh55178	FXOS : Processus svc_sam_dcosAG plante sans arrêt sur FirePower 4100
CSCwh68077	Changements de Jitterentropy dans les versions de LTS18 et versions ultérieures ce qui provoque l'échec de la version de FTD
CSCwh99041	CCM, séq. 57 – LTS21
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
CSCwi34600	Connexion par clé du protocole SSH ne fonctionne pas dans ASAv dans lequel la configuration par défaut sur GCP est chargée
CSCvx44261	SNMPv3 : les caractères spéciaux utilisés dans la configuration SNMPv3 de FXOS provoquent des erreurs d'authentification
CSCwc60800	CIAM : noyau linux 5.10.1.79 CVE-2022-30594
CSCwc65508	CIAM : libtirpc – CVE-2021-46828
CSCwc76419	Journaux d'erreur inutiles du ventilateur doivent être supprimés du fichier thermique

Identifiant	En-tête :
CSCwc78220	CIAM : zlib – CVE-2022-37434
CSCwd22389	Vulnérabilités dans SQLite – CVE-2022-35737 et autres
CSCwd81123	Utilisation élevée du processeur sur FXOS pour les processus smConlogging
CSCwe21884	Rédaction d'enveloppe autour de la commande « kill » pour journaliser qui l'appelle
CSCwe42949	Installation de l'outil « perf » dans FXOS pour FTD.
CSCwe70472	Mise à niveau du composant tiers rng-tools à la dernière version 6.16
CSCwe81837	FXOS : Ajout de tracefs dans la version lancée
CSCwf22483	SSH vers châssis permet une prise de contact tridirectionnelle pour les adresses IP qui ne sont pas autorisées par la configuration
CSCwf36066	WM/TPK/WA « FTD only » : Pertes de paquets observées après le retrait du membre du PC du canal de port
CSCwf38253	Ajouter iotop aux sites avec version de FXOS antérieure à FXOS 2.14
CSCwf44354	JENT : Extension de prise en charge de la bibliothèque JENT à CiscoSSL pour toutes les cibles FXOS
CSCwf63589	Recherche de la source et redémarrage pour le processus snmpd sur Cisco FTD
CSCwf78950	Processus FMC ssp_snmp_trap_fwdr entraîne une utilisation élevée de la mémoire
CSCwf79552	Évite l'échec au niveau du démarrage de RADWARE dans FXOS 2.13 à compter de juin 2024
CSCwf85946	Option tCAM de la commande de journalisation de débogage ne fonctionne pas sur wm1010
CSCwf92512	Volume compatible avec FXOS.sh manquant dans les succursales avec une version antérieure à R2140
CSCwf95888	FPR1K Switchport transmet le trafic CDP
CSCwf98469	Suppression de l'ancienne version d'iotop 0.6
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.
CSCwh03488	Erreur lors du nettoyage du mappage du port physique pour tous les ports du TPK
CSCwh06501	Authentification externe SSH FTD affiche « \pam_radius verify_packet: Bad code\ » 7.4.0-1928
CSCwh22888	FXOS : Suppression de l'application de l'état dégradé des lames après plusieurs erreurs corrigibles de DIMM

Identifiant	En-tête :
CSCwh30172	Tampon de validation ne doit pas être désactivé en mode appareil pour la fonction de détection de fuite de mémoire UCSM
CSCwh35138	Pendant le processus de redémarrage par effacement sécurisé, le message d'erreur ERROR: Timeout Attending for FXos_log_shutdown a été observé.
CSCwh70735	Ajout de la bibliothèque jemalloc aux unités de Cisco FTD
CSCwh91941	En mode débogage de LTP, lors de l'exécution de « show_mgmt_port », l'adresse inet est manquante
CSCwi20690	Revmove pour recette HTMLDOC locale
CSCwi24668	CCM, séq. 59 – LTS21
CSCwi26273	WM RM : 100 % d'utilisation du processeur du système pour le cœur 0 sur la plateforme WM
CSCwe34512	JENT : Ajout de la bibliothèque JENT à fxos pour prendre en charge KP
CSCwf36750	Mise à niveau du composant lldpd à la version 1.0.16
CSCwh08839	Suppression du correctif local CSCwh06501.patch une fois qu'il a été géré par CCM
CSCwh71202	Mise à jour des scripts CIAM sur FXOS
CSCwh99707	Mise à jour des scripts CIAM pour inclure l'ID CVE dans les attributs et ajouter l'attribut WR_CASE_PENDING
CSCwi49448	Mise à jour de l'infrastructure de la couche CCM
CSCwi61028	Script de remplissage de bogues CIAM sur FXOS n'attend pas que le bogue soit signalé
CSCwf33115	Ajout de la prise en charge de 7zip dans FMC
CSCwh33196	SSP MIO : prise en charge du jeton Swims dans l'image de signature
CSCwh58010	Désactivation de CL3420025 de fxplatform/liverpool/FXOS_2_10_1à

Bogues résolus dans la version FXOS 2.13.0.243

Le tableau suivant répertorie les bogues déjà indiqués dans la version précédente et trouvés par le client, puis résolus dans FXOS 2.13.0.243 :

Identifiant	En-tête :
CSCwe95747	724-118 : portmgr_discover_epm : échec de découverte de la carte – échec de détection du type de carte EPM
CSCvx99187	Échec de définition du DNS, du nom d'hôte et de l'adresse IP sur TPK 3130.
CSCwc83495	Ajout de la commande abort dans switch_driver pour faire planter le portmanager lorsque les udbs sont corrompus

Identifiant	En-tête :
CSCwd10822	Déclencheur de basculement en raison de la défaillance du moteur d'inspection de l'autre unité à cause d'une défaillance du disque
CSCwd34888	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
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)
CSCwd90894	Appareils de sécurité adaptables Cisco : Impossible de se connecter par SSH à l'interface après la mise à niveau.
CSCwd94181	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
CSCwd96493	Link Up visible pendant quelques secondes sur FPR1010 pendant le démarrage.
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
CSCwd99885	Mauvais changement de code pour portmgr_ipc.c
CSCwe13615	Échec intermittent de l'instance d'application lors de l'installation.
CSCwe15477	Port TPK MGMT n'est pas en mesure d'envoyer un message Ping à la passerelle après l'installation de l'application
CSCwe22176	Mise à jour de l'identifiant de validation WR6, WR8, LTS18 et LTS21 dans la couche CCM (séq. 43)
CSCwe24532	Plusieurs instances des fichiers journaux nvram.out ont fait l'objet d'une rotation sous /opt/cisco/platform/logs/
CSCwe25593	Lecteur en double du registre de réinitialisation comme solution de contournement en cas de réinitialisation aléatoire aux valeurs d'usine
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
CSCwe30567	Solution de contournement pour définir hwclock à partir des journaux de ntp sur les plates-formes bas de gamme
CSCwe32394	abort/reload ssp : Arrêt appelé après le lancement d'une instance de « Stb::ad_alloc » à partir de la commande surcharge.cpp
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

Identifiant	En-tête :
CSCwe39425	2100 : La bascule du commutateur entraîne des arrêts accidentels et une réinitialisation « PowerCycleRequest ».
CSCwe46036	Périphériques FP1K/2K/3K ne peuvent pas recevoir le trafic de monodiffusion
CSCwe51412	Canal de port inactif avec état suspendu sur les ports membres
CSCwe59809	Mise à jour de l'ID de validation WR6, WR8, LTS18 et LTS21 dans la couche CCM (séq. 45)
CSCwe64773	Fichier core.svc_sam_dcosAG observé sur l'appareil après l'effacement de la configuration
CSCwe72535	Connexion impossible au FTD par l'authentification extérieure
CSCwe74059	logrotate ne compresse pas les fichiers sur les appareils de sécurité adaptables Cisco 9.16 ou sur FTD 7.0.
CSCwe74916	Interface HORS SERVICE dans un ensemble en ligne avec état propagate pour le lien
CSCwe83544	Après la mise à niveau, l'interface ha reste bloquée sur un nœud
CSCwe88600	Plantage silencieux de vFTD sshd, probablement dû aux sondes avec LB dans Azure
CSCwe89731	Notification de fausse alarme envoyée par le démon pour panne de service.
CSCwe93802	Mise à jour de l'identifiant de validation WR6, LTS18 et LTS21 dans la couche CCM (séq. 46)
CSCwf01306	WM : Fichier principal LINA tronqué
CSCwf02779	Après la mise à mise à niveau des appareils de sécurité adaptables Cisco, le périphérique passe en mode sécurisé après affichage de l'erreur « fxos_api_xml_decode: XML_Parse return error ».
CSCwf03714	Annulation des modifications apportées à CSCwd89848 sur FXOS pour éviter tout problème de compatibilité de versions entre FXOS et LINA.
CSCwf04983	Échec d'ajout de l'unité 3100 à la grappe avec l'erreur « configured object (sys/switch-A/slot-2) not found ».
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 »
CSCwf14729	Nécessité d'utiliser CiscoSSL avec FOM 7.3 pour les versions d'Intel
CSCwf7858	Noeud quitte la grappe TPK en raison d'un échec du contrôle d'intégrité de l'interface
CSCwf18428	KP/WM : État de fonctionnement de l'interface de gestion toujours actif, même après la commande « shut ».
CSCwf18875	Connexion SSH ne fonctionne pas après la mise à niveau de 99-18-1-866 vers 99-20-0-245.

Identifiant	En-tête :
CSCwf51933	Échec de connexion par authentification extérieure pour le AAA-RADIUS après la mise à mise à niveau
CSCwf59098	Mise à jour de l'identifiant de validation LTS21 dans la couche CCM (séq. 49)
CSCwf59643	[IMS_7_4_0] KP à haute disponibilité désactivé après le redémarrage : Erreur de synchronisation de l'application du CD - échec d'application de la configuration du SSP en veille
CSCwf65396	Mise à jour de l'ID de validation WR6, WR8, LTS18 et LTS21 dans la couche CCM (séq. 50)
CSCvx71936	FXOS : Défaillance « The password encryption key has not been set. » affichée sur les appareils FPR1000 et FPR2100
CSCwb23251	Noyau sspos_snmp_suba observé lors du test de longévité sur FP1K
CSCwb67524	TPK : Échec d'affichage des ports réseau ouverts en mode de déploiement de conteneur
CSCwc10545	system_rid_specic_misc_defs.json a des cœurs système incorrects pour TPK
CSCwc34801	[IMS_7_3_0]REST_API:Network::getMTU [ERROR] au moment de définir les détails du réseau lors du premier démarrage
CSCwc69977	Vérification du pointeur nul manquant dans la routine d'affichage sfp
CSCwc83851	Erreurs OIR dans portmgr.out
CSCwd07098	SFP 25G CU ne fonctionne pas en netmod 8x25G dans Brentfield
CSCwd10880	Alertes d'intégrité critiques « user configuration(FSM.sam.dme.AaaUserEpUpdateUserEp) » sur les périphériques 2100/3100.
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
CSCwd59785	Utilisation de freeradius-client fourni par Wind River
CSCwd59807	Utilisation des ghostscript-fonts fournies par Wind River.
CSCwd67101	FPR1150 : Erreur de format d'exécution constatée et appareil bloqué jusqu'au rechargement, après exécution de « secure all »

Identifiant	En-tête :
CSCwd68159	LLDP : Suppression d'un port membre du canal de port supprime complètement les voisins lldp
CSCwd70490	Indicateur d'état du port du membre du canal de port et état d'adhésion sont inactifs lorsqu'aucun LACPDU n'a été reçu
CSCwd80343	MI FTD exécutant la version 7.0.4 indique une utilisation de disque élevée
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
CSCwe00662	Création d'un local_User non verrouillée même après avoir défini le nombre maximal de tentatives de connexion
CSCwe02421	FPR-X-NM-6X1SX-F non reconnu sur FP3100 ou FP4200
CSCwe201569	Amélioration des options de l'interface de ligne de commande la gestion de l'IP avec l'option DHCP
CSCwe22252	Cœurs SNMPD vus dans in snmp_sess_Close et notifyTable_register_notifications
CSCwe22302	Partition « /opt/cisco/config » est pleine en raison d'une rotation insuffisante du journal du fichier wtmp
CSCwe25314	Actualisation du fichier ios.pem.
CSCwe32972	stdout_env_manager.log est rempli de messages de tableau de type 3 inconnus
CSCwe33699	stdout_00aa_ssp_syslog.log est rempli de messages sur crond
CSCwe36758	3105 : F78672 après un redémarrage
CSCwe47278	Authentification externe SSH affiche « pam_radius verify_packet: Bad code » avec radius 7.4.0-1672
CSCwe48918	LTS18 CCM numéro de séquence 44 pour mettre à mettre à jour la libjitterentropy à la version 3.4.1
CSCwe49436	Niveau du journal par défaut de WM est réglé à critique
CSCwe50946	État de la liaison de l'interface de gestion non synchronisé entre FXOS et l'appareil de sécurité adaptable Cisco
CSCwe50993	SNMP sur le module SFR s'éteint et ne se rallume pas
CSCwe53429	Commande « create device-manager » bloquée en mode natif ASA/FTD
CSCwe63794	Réduction du niveau de gravité des défaillances pour la dégradation RAID en raison d'un disque toujours en état de rechange
CSCwe72322	Mises en garde hebdomadaires du logiciel Coverity System SA 2023-03-20, défauts 878323 pour Coverity

Identifiant	En-tête :
CSCwe73070	Sur WA/TPK, lorsque management1/1 est en panne, le diagnostic lina en mode CMI et non-CMI est activé
CSCwe81114	TPK-CCmode : Erreur : tamm_espi_read 0, 0xb2c000: 769-TAM_ERROR_DEVICE_NOT_REGISTERED
CSCwe81695	logger.1 : échec d'envoi du message : les journaux des ressources temporairement indisponibles ont été vus après le rechargement de la version 7.2.4-94
CSCwe83962	Informations sur LLDP::Neighbors ne sont pas découvertes sur tous les ports membres d'une interface de canal de port
CSCwe90524	Amélioration : Ajout d'un horodatage dans le message IPC de l'interface
CSCwe93202	API REST FXOS : Impossible de créer un trousseau de clés de type « ecdsa ».
CSCwe93736	Appareil de sécurité adaptable Cisco ne met pas à jour le fuseau horaire malgré les commandes.
CSCwe96450	2100 : Vérification de l'état d'exécution de poshd dans FXOS 2.13/2.14 pour les arrêts progressifs par commutation de l'interrupteur d'alimentation
CSCwf03241	Perte de l'accès de gestion au 3110 (mode natif)
CSCwf03490	portmanager.sh affiche les avertissements bash continus dans les fichiers journaux
CSCwf06042	Limitation de vitesse des interfaces membres de PC n'a pas été mise à jour après le renvoi d'OIR dans ECM
CSCwf1187	TPK 3110 – INCOMPATIBILITÉ de la version du micrologiciel après la mise à niveau à la version 7.2.4-144.
CSCwf12814	Problème de version de python3-funcsigs avec LTS21
CSCwf21669	Bibliothèque jemalloc requise dans le système d'exploitation windriver
CSCwf2887	FXOS : Commande « show portchannel summary » affiche des interfaces incorrectes lors de l'utilisation de ports d'éclatement
CSCwf35385	Correction du nom de la recettes CiscoSSL dans R2130
CSCwf36083	Affichage de la commande du menu 4 de débogage de SNMP dans le cadre de l'affichage technique FPRM pour FTD.
CSCwf37887	Passage à la version 1.19.4 dans les succursales LTS21
CSCwf40113	TPK/WA – Paquets OSPF arrivent dans plusieurs boucles RX
CSCwf43140	port-manager : devNum 0 n'a pas initialisé le module fwd
CSCwf43817	Prise en charge de KC25/KC50 pour le micrologiciel 0x500_000a
CSCwf50358	FCM : Bibliothèque jacoco doit être mise à niveau

Identifiant	En-tête :
CSCwf59176	FXOS déclenche une défaillance pour l'interface de gestion désactivée par l'administrateur
CSCwf60483	Inondation dans le journal DME dans certains scénarios
CSCwf73773	Code manquant dans la capture de vidage de RMU
CSCwf75568	Modifications de Livecore pour prendre en charge la fonction d'instantané en direct
CSCwf80895	Mise à jour de l'identifiant de validation LTS21 dans la couche CCM (séq. 52)
CSCwb05555	Modification des paramètres de squelch de Brentwood et de Maryland
CSCwe24440	Description de suppression du contrôleur de disque remove/remove-secure ne correspond pas
CSCwe33273	3100 : Erreurs Insmod observées sur la console
CSCwf19647	Modification des paramètres de squelch de Brentwood et de Maryland manquante dans les variantes _X netmod
CSCwf8655	Les p4tickets universels sont en texte brut dans le code source
CSCwf55787	Retravail de la recette CiscoSSL
CSCvz69950	Amélioration : Inclure la sortie de la commande « show storage detail » dans le fichier FPR3100 FPRM/tech_support_brief
CSCwb06934	Amélioration : Inclure la sortie de la commande « show slot expand detail » dans le fichier tech_support_brief du FPR3100
CSCWC12716	Modification de l'assistance technique pour obtenir des informations de débogage supplémentaires (détails du registre de liaison de contrôle)
CSCwd83015	Amélioration à TPK/WA – Ajout de la commande « show tail-drop-allocated buffers all » à LuaCLI de Marvel pour le soutien technique
CSCwe42455	Configuration des événements par défaut pour l'amélioration des diagnostics des commutateurs
CSCwe69220	Mise à jour des scripts Corone CIAM
CSCwe73826	Amélioration : Inclusion de l'ID de port Ethernet dans la commande « show portmanager switch commutateur status »
CSCwe79517	Amélioration : TPK affiche les compteurs du gestionnaire de ports pour vidanger les compteurs des règles de rejet par défaut
CSCwe87873	Exigence : L'utilitaire de rotation des journaux doit gérer la rotation du fichier asa-appagent.log
CSCwe89534	Activation de la journalisation de débogage pour le pilote du commutateur WM-1010

Identifiant	En-tête :
CSCwf03345	Récupération après des défaillances de RMU en raison du mauvais état du lien de contrôle
CSCwf23077	Amélioration : Migration de la rotation des journaux fover trace vers l'utilitaire logrotate de FXOS
CSCwf23213	WM RM – Diagnostics des commutateurs – Événements, journalisation et action
CSCwf49700	WA/tpk : Modifications à FXOS pour la prise en charge unifiée de la capture de paquets pour l'enregistrement des paquets abandonnés par le commutateur
CSCwf79947	Correction d'un problème de version des outils de compactage du micrologiciel en raison d'un changement dans la version de python
CSCwd90889	Mise à niveau de Perforce nécessite des modifications à l'emplacement de définition de P4PORT
CSCwe58542	suppression du hachage à la fin de la version de Marvel

Bogues résolus dans la version FXOS 2.13.0.212

Le tableau suivant répertorie les bogues déjà indiqués dans la version précédente et trouvés par le client, puis résolus dans FXOS 2.13.0.212 :

Numéro d'identification de la mise en garde	Description
CSCwd34662	Mise à jour de l'identifiant de validation LTS18 et LTS21 dans la couche CCM (séq. 39)
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)
CSCwe09956	cdc_ether.ko manquant dans les versions de FMC basées sur LTS21
CSCwd21325	FPR 3100 : Commande « show local-user detail » avec erreur « Error opening the tally file »
CSCwb66175	Enregistrement du MIO impossible, problème associé au processus appAG
CSCwc50267	MIO LTS21 : libcurl.so.4.7.0 redondante à l'élagage
CSCwd06758	Aucune validation d'entrée pour les serveurs DNS des appareils logiques dans la configuration de démarrage sur le gestionnaire de châssis
CSCwd47340	Fuite de mémoire potentielle dans le processus svc_sam_envAG
CSCwd50036	WA_B/TPK. SFP double plage (10/25) ne fonctionne pas avec netmod 8 * 10g avec vitesse détectée par sFP

Numéro d'identification de la mise en garde	Description
CSCwd56654	Défaillances de plateforme liées à l'interface de gestion
CSCwd74282	Appareil 3100 passe en mode de sécurité intégrée en raison d'une incompatibilité de version du NPU
CSCwb52656	Journaux de suivi SNM ont des horodatages incorrects
CSCwc38737	disk-0 local affiché sur fpr9300
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

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.