

Redémarrage inattendu du pare-feu sécurisé en raison d'un problème de déchargement de flux DTLS

Table des matières

Problème

Cisco Secure Firewall Threat Defense (FTD) redémarre le système, ce qui entraîne des interruptions de service répétées et ne génère pas de fichiers crashinfo traditionnels. Lors du dépannage, la génération répétée de fichiers `crypto_eng0_arch_*` est observée, ainsi que des messages d'erreur fatale NPU et FPGA récurrents qui coïncident avec les événements de redémarrage.

- Le répertoire FTD confirme la génération répétée de fichiers `crypto_eng0_arch_*` avec des horodatages coïncidant avec des événements de redémarrage.

```
firepower# dir crypto_archive
-rwxr-xr-x 1 root root 55310816 Mar 12 01:22 crypto_eng0_arch_1.bin
-rwxr-xr-x 1 root root      869 Mar 12 01:22 crypto_eng0_arch_1.info
-rwxr-xr-x 1 root root  409235 Mar 12 01:22 crypto_eng0_arch_1.reg
-rwxr-xr-x 1 root root 55310816 Mar 12 04:25 crypto_eng0_arch_2.bin
-rwxr-xr-x 1 root root      869 Mar 12 04:25 crypto_eng0_arch_2.info
-rwxr-xr-x 1 root root  409111 Mar 12 04:25 crypto_eng0_arch_2.reg
-rwxr-xr-x 1 root root 55310816 Mar 12 09:45 crypto_eng0_arch_3.bin
-rwxr-xr-x 1 root root      869 Mar 12 09:45 crypto_eng0_arch_3.info
-rwxr-xr-x 1 root root  408688 Mar 12 09:44 crypto_eng0_arch_3.reg
-rwxr-xr-x 1 root root 55310816 Mar 11 18:48 crypto_eng0_arch_4.bin
-rwxr-xr-x 1 root root      869 Mar 11 18:48 crypto_eng0_arch_4.info
-rwxr-xr-x 1 root root  408895 Mar 11 18:48 crypto_eng0_arch_4.reg
-rwxr-xr-x 1 root root 55310816 Mar 11 21:11 crypto_eng0_arch_5.bin
-rwxr-xr-x 1 root root      869 Mar 11 21:11 crypto_eng0_arch_5.info
-rwxr-xr-x 1 root root  409136 Mar 11 21:11 crypto_eng0_arch_5.reg
```

- Les journaux FTD affichent des messages d'erreur fatale FPGA et d'accélérateur NPU récurrents qui correspondent à la durée des redémarrages inattendus et des fichiers `crypto_eng0_arch_*`.

```

> expert
admin@device:~$ sudo su
Password: [enter admin password]
root@device:/Volume/home/admin# cat /opt/cisco/platform/logs/messages | grep -i npu
2026 Mar 11 07:11:42 KC FPGA: FATAL - ILK pipe 0: TX Buffer FIFO Overflow
2026 Mar 11 07:11:42 NPU ACCEL MGR: FATAL - NPU Accelerator FAILED
2026 Mar 11 07:11:42 NPU ACCEL MGR: FATAL - NPU Accelerator FAILED - REBOOTING the device !!
2026 Mar 11 11:15:47 KC FPGA: FATAL - ILK pipe 0: TX Buffer FIFO Overflow
2026 Mar 11 11:15:47 NPU ACCEL MGR: FATAL - NPU Accelerator FAILED
2026 Mar 11 11:15:47 NPU ACCEL MGR: FATAL - NPU Accelerator FAILED - REBOOTING the device !!
---
Mar 11 21:11:20 device kings-cross-fpga: FATAL - ILK pipe 0: TX Buffer FIFO Overflow
Mar 11 21:11:20 device NPU Accelerator Manager: FATAL - NPU Accelerator FAILED
Mar 11 21:11:20 device FPRM: <<%FPRM-2-NPU_FPGA_FAILURE>> [F1418][critical][npu-fpga-failure][sha
Mar 11 21:11:20 device NPU Accelerator Manager: FATAL - NPU Accelerator FAILED - REBOOTING the de
Mar 12 01:22:53 device kings-cross-fpga: FATAL - ILK pipe 0: TX Buffer FIFO Overflow
Mar 12 01:22:54 device NPU Accelerator Manager: FATAL - NPU Accelerator FAILED
Mar 12 01:22:54 device FPRM: <<%FPRM-2-NPU_FPGA_FAILURE>> [F1418][critical][npu-fpga-failure][sha
Mar 12 01:22:54 device NPU Accelerator Manager: FATAL - NPU Accelerator FAILED - REBOOTING the de

```

- La configuration FTD confirme que le déchargement de flux DTLS est activé sur le FTD affecté, ce qui correspond aux conditions pour le défaut connu ID de bogue Cisco CSCwq32085.

```

firepower# show flow-offload-dtls info
DTLS offload: Enabled
Egress optimization: Enabled

```

Environnement

- Principalement visible sur la gamme Firepower 3100, mais a un impact sur les autres modèles
- Affecte les ASA et les FTD qui ne sont pas sur une version fixe pour le problème.
- Géré par Firepower Management Center (FMC)
- Déchargement de flux DTLS activé sur les périphériques affectés

Résolution

Mettez à niveau tous les appareils FTD/ASA affectés vers une version incluant le correctif du bogue Cisco défectueux ayant l'ID [CSCwq32085](#).

Solution de contournement

1. Accédez à Devices > FlexConfig dans Cisco Secure Firewall Management Center.
2. Créez ou modifiez un objet FlexConfig.
3. Insérez le texte de ligne de commande pour désactiver le déchargement de flux DTLS/IPSEC pour le périphérique FTD via FlexConfig.

```
no flow-offload-ipsec  
no flow-offload-dtls
```

4. Attribuez la politique FlexConfig au périphérique FTD ciblé et déployez la configuration.
5. La modification nécessite un redémarrage FTD pour que les modifications soient prises en compte.

Motif

Les redémarrages inattendus ont été provoqués par l'ID de bogue Cisco CSCwq32085 dans FTD. Ce défaut logiciel connu peut déclencher des pannes d'accélérateur NPU/FPGA et des redémarrages forcés lorsque le délestage de flux DTLS est activé sur les appliances des gammes Firepower 3100 et 4200. Le défaut affecte spécifiquement les fonctions d'accélération matérielle et génère des fichiers crypto_archive avec un message d'erreur de console "Problème KC ILK détecté" avant de forcer le redémarrage du système.

Autres informations utiles

- [Comprendre et dépanner le déchargement IPsec et DTLS dans Secure Firepower 3100 et](#)

[4200](#)

- [Configuration des objets FlexConfig](#)
- [ID de bogue Cisco CSCwq32085](#)
- [Notes de version de Cisco Secure Firewall Threat Defense, version 7.6.x](#)
- [Assistance technique de Cisco et téléchargements](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.