

DTLSフローオフロードの問題により、セキュアファイアウォールが予期せずリブートする

内容

問題

Cisco Secure Firewall Threat Defense(FTD)でシステムのリブートが発生すると、サービスが中断が繰り返し発生し、従来のcrashinfoファイルが生成されません。トラブルシューティング中、再起動イベントと一致するNPUアクセラレータとFPGAの致命的なエラーメッセージが繰り返し表示され、crypto_eng0_arch_*ファイルが繰り返し生成されます。

- FTDディレクトリで、再起動イベントと一致するタイムスタンプを持つ crypto_eng0_arch_*ファイルが繰り返し生成されたことが確認されます。

```
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
```

- FTDログには、予期しないリブートのタイミングとcrypto_eng0_arch_*ファイルに一致する、繰り返し発生するNPUアクセラレータおよびFPGAの致命的なエラーメッセージが表示されます。

```
> 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

```

- FTDの設定では、該当するFTDでDTLSフローオフロードが有効であることが確認されています。これは、既知の不具合のCisco Bug ID CSCwq32085の条件に一致します。

```

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

```

環境

- 主にFirepower 3100シリーズで使用されているが、他のモデルに影響を与える
- この問題の修正済みバージョンではないASAおよびFTDに影響します。
- Firepower Management Center(FMC)による管理
- 影響を受けるデバイスで有効にされたDTLSフローオフロード

解決方法

該当するすべてのFTD/ASAアプライアンスを、不具合Cisco Bug ID [CSCwq32085](#)の修正を含むバージョンにアップグレードします。

回避策

1. Cisco Secure Firewall Management Centerで、Devices > FlexConfigの順に選択します。
2. FlexConfigオブジェクトを作成または編集します。
3. コマンドラインテキストを挿入して、FlexConfigを介したFTDデバイスのDTLS/IPSECフローオフロードを無効にします。

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

4. ターゲットのFTDデバイスにFlexConfigポリシーを割り当て、設定を展開します。
5. 変更を有効にするには、FTDをリブートする必要があります。

原因

予期しないリブートは、FTDのCisco Bug ID CSCwq32085が原因で発生しました。この既知のソフトウェア不具合は、Firepower 3100および4200シリーズアプライアンスでDTLSフローオフロードが有効になっている場合に、NPU/FPGAアクセラレータの障害を引き起こし、強制的なリブートを引き起こす可能性があります。この不具合は、特にハードウェアアクセラレーション機能に影響を与え、「KC ILK issue detected」コンソールエラーメッセージを含むcrypto_archiveファイルを生成してから、システムを強制的にリブートします。

関連コンテンツ

- [Secure Firepower 3100および4200のIPSecおよびDTLSオフロードの説明とトラブルシューティング](#)
- [FlexConfigオブジェクトの設定](#)
- [Cisco Bug ID CSCwq32085](#)

- [Cisco Secure Firewall Threat Defenseリリースノート、バージョン7.6.x](#)
- [シスコのテクニカルサポートとダウンロード](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。