

Sichere Firewall wird aufgrund eines DTLS-Flow-Offload-Problems unerwartet neu gestartet

Inhalt

Problem

Die Cisco Secure Firewall Threat Defense (FTD) wird vom System neu gestartet, was wiederholt zu Serviceunterbrechungen führt, ohne dass herkömmliche Abstürze von Dateien auftreten. Während der Fehlerbehebung wird eine wiederholte Generierung von `crypto_eng0_arch_*`-Dateien beobachtet, zusammen mit wiederkehrenden NPU-Accelerator- und FPGA-Fehlermeldungen, die mit den Neustartereignissen zusammenfallen.

- Das FTD-Verzeichnis bestätigt die wiederholte Generierung von `crypto_eng0_arch_*`-Dateien mit Zeitstempeln, die mit Neustartereignissen übereinstimmen.

```
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-Protokolle zeigen sich wiederholende Fehlermeldungen zum NPU-Beschleuniger und FPGA mit schwerwiegenden Folgen, die mit dem Zeitpunkt unerwarteter Neustarts und `crypto_eng0_arch_*`-Dateien übereinstimmen.

> 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

```

- Die FTD-Konfiguration bestätigt, dass der DTLS-Fluss-Offload auf dem betroffenen FTD aktiviert ist, was den Bedingungen für den bekannten Fehler Cisco Bug-ID CSCwq32085 entspricht.

```

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

```

Umwelt

- Hauptsächlich bei Firepower der Serie 3100 zu beobachten, wirkt sich jedoch auf andere Modelle aus
- Auswirkungen auf ASAs und FTDs, die nicht auf einer festen Version des Problems vorhanden sind.
- Verwaltet von FirePOWER Management Center (FMC)
- DTLS-Flow-Offload auf betroffenen Geräten aktiviert

Auflösung

Führen Sie für alle betroffenen FTD/ASA-Appliances ein Upgrade auf eine Version durch, die die Fehlerbehebung für die Cisco Bug-ID [CSCwq32085](#) enthält.

Problemumgehung

1. Gehen Sie zu Devices > FlexConfig im Cisco Secure Firewall Management Center.
2. Erstellen oder bearbeiten Sie ein FlexConfig-Objekt.
3. Fügen Sie den Befehlszeilentext ein, um DTLS/IPSEC-Flow Offload für das FTD-Gerät über FlexConfig zu deaktivieren.

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

4. Weisen Sie die FlexConfig-Richtlinie dem FTD-Zielgerät zu, und stellen Sie die Konfiguration bereit.
5. Die Änderung erfordert einen FTD-Neustart, damit die Änderungen wirksam werden.

Ursache

Die unerwarteten Neustarts wurden durch die Cisco Bug-ID CSCwq32085 in FTD verursacht. Dieser bekannte Softwarefehler kann NPU/FPGA-Beschleunigungsfehler auslösen und einen erzwungenen Neustart auslösen, wenn die DTLS-Flussauslagerung auf den Firepower-Appliances der Serien 3100 und 4200 aktiviert ist. Der Defekt betrifft speziell die Hardware-Beschleunigungsfunktionen und erzeugt crypto_archive-Dateien mit einem "KC ILK Problem entdeckt" Konsolen-Fehlermeldungen, bevor das System neu startet.

Verwandte Inhalte

- [IPsec- und DTLS-Offloading in Secure Firepower 3100 und 4200 analysieren und Fehler](#)

beheben

- [Konfigurieren von FlexConfig-Objekten](#)
- [Cisco Bug-ID: CSCwq32085](#)
- [Cisco Secure Firewall Threat Defense - Versionshinweise, Version 7.6.x](#)
- [Technischer Support und Downloads von Cisco](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.