

Riavvii imprevisti del firewall protetto a causa di un problema di offload del flusso DTLS

Sommario

Problema

Cisco Secure Firewall Threat Defense (FTD) prevede il riavvio del sistema, che causa ripetutamente interruzioni del servizio e senza generare i tradizionali file crashinfo. Durante la risoluzione dei problemi, viene osservata la generazione ripetuta di file `crypto_eng0_arch_*` insieme ai messaggi di errore irreversibile ricorrenti dell'acceleratore NPU e FPGA che coincidono con gli eventi di riavvio.

- La directory FTD conferma la generazione ripetuta di file `crypto_eng0_arch_*` con timestamp che coincidono con gli eventi di riavvio.

```
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
```

- I log FTD mostrano i messaggi di errore irreversibili ricorrenti dell'acceleratore NPU e FPGA che corrispondono ai tempi dei riavvii imprevisti e dei file `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 configurazione FTD conferma che l'offload del flusso DTLS è abilitato sull'FTD interessato, che soddisfa le condizioni per l'ID bug Cisco noto CSCwq32085.

```

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

```

Ambiente

- Visibile principalmente su Firepower serie 3100, ma influisce su altri modelli
- Ha impatto su ASA e FTD che non sono su una versione fissa per il problema.
- Gestito da Firepower Management Center (FMC)
- Offload del flusso DTLS abilitato sui dispositivi interessati

Risoluzione

Aggiornare tutti gli accessori FTD/ASA interessati a una versione che includa la correzione per il bug Cisco con ID [CSCwq32085](#).

Soluzione alternativa

1. Andare a Devices > FlexConfig in Cisco Secure Firewall Management Center.
2. Creare o modificare un oggetto FlexConfig.
3. Inserire il testo della riga di comando per disabilitare DTLS/IPSEC Flow Offload per il dispositivo FTD tramite FlexConfig.

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

4. Assegnare il criterio FlexConfig al dispositivo FTD di destinazione e distribuire la configurazione.
5. Affinché le modifiche abbiano effetto, è necessario riavviare l'FTD.

Causa

I riavvii imprevisti sono stati causati da un bug Cisco con ID CSCwq32085 in FTD. Questo noto difetto del software può causare guasti all'acceleratore NPU/FPGA e riavvii forzati quando l'offload del flusso DTLS è abilitato sulle appliance Firepower serie 3100 e 4200. Il difetto influisce in modo specifico sulle funzioni di accelerazione hardware e genera file crypto_archive con messaggi di errore della console "Rilevato problema di KC" prima di forzare il riavvio del sistema.

Contenuto correlato

- [Comprensione e risoluzione dei problemi di offload IPsec e DTLS in Secure Firepower 3100 e 4200](#)
- [Configurazione degli oggetti FlexConfig](#)
- [ID bug Cisco CSCwq32085](#)

- [Note sulla versione di Cisco Secure Firewall Threat Defense, versione 7.6.x](#)
- [Supporto tecnico Cisco e download](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).