

Secure Firewall Unexpectedly Reboots Due to DTLS Flow Offload Issue

Contents

Issue

Cisco Secure Firewall Threat Defense (FTD) experiences system reboots, repeatedly causing service disruption and without generating traditional crashinfo files. During troubleshooting, repeated generation of `crypto_eng0_arch_*` files is observed along with recurring NPU accelerator and FPGA fatal error messages that coincide with the reboot events.

- FTD directory confirms repeated generation of `crypto_eng0_arch_*` files with timestamps coinciding with reboot events.

```
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 logs show recurring NPU accelerator and FPGA fatal error messages that match the timing of unexpected reboots and `crypto_eng0_arch_*` files.

```
> 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 configuration confirms that DTLS flow offload is enabled on the affected FTD, which matches the conditions for known defect Cisco bug ID CSCwq32085.

```

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

```

Environment

- Mainly seen on Firepower 3100 series, but impacts other models
- Impacts ASAs and FTDs that are not on a fixed version for the issue.
- Managed by Firepower Management Center (FMC)
- DTLS flow offload enabled on affected devices

Resolution

Upgrade all affected FTD/ASA appliances to a version which includes the fix for defect Cisco bug ID [CSCwq32085](#).

Workaround

1. Go to **Devices > FlexConfig** in the Cisco Secure Firewall Management Center.

2. Create or edit a **FlexConfig Object**.

3. Insert the command line text to disable DTLS/IPSEC Flow Offload for the FTD device via FlexConfig.

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

4. Assign the **FlexConfig Policy** to the targeted FTD device and deploy the configuration.

5. The change requires an FTD reboot for the changes to take affect.

Cause

The unexpected reboots were caused by Cisco bug ID **CSCwq32085** in FTD. This known software defect can trigger NPU/FPGA accelerator failures and forced reboots when DTLS flow offload is enabled on Firepower 3100 and 4200 series appliances. The defect specifically affects the hardware acceleration features and generates crypto_archive files with a "KC ILK issue detected" console error messages before forcing system reboots.

Related Content

- [Understand and Troubleshoot IPsec and DTLS Offloading in Secure Firepower 3100 and 4200](#)
- [Configuring FlexConfig Objects](#)
- [Cisco bug ID CSCwq32085](#)
- [Cisco Secure Firewall Threat Defense Release Notes, Version 7.6.x](#)
- [Cisco Technical Support & Downloads](#)