

Firewall seguro se reinicia inesperadamente debido a un problema de descarga de flujo DTLS

Contenido

Problema

Cisco Secure Firewall Threat Defence (FTD) se reinicia el sistema, lo que provoca repetidamente interrupciones en el servicio y sin generar los archivos crashinfo tradicionales. Durante la resolución de problemas, se observa la generación repetida de archivos `crypto_eng0_arch_*` junto con los mensajes de error irre recuperables recurrentes del acelerador NPU y FPGA que coinciden con los eventos de reinicio.

- El directorio FTD confirma la generación repetida de archivos `crypto_eng0_arch_*` con marcas de tiempo que coinciden con los eventos de reinicio.

```
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
```

- Los registros de FTD muestran mensajes de error irre recuperables recurrentes del acelerador NPU y FPGA que coinciden con el tiempo de reinicios inesperados y los archivos `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 configuración de FTD confirma que la descarga de flujo de DTLS está habilitada en el FTD afectado, que coincide con las condiciones para el ID de bug de Cisco CSCwq32085 conocido como defectuoso.

```

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

```

Entorno

- Se observa principalmente en Firepower serie 3100, pero afecta a otros modelos
- Afecta a los ASA y FTD que no están en una versión fija para el problema.
- Administrado por Firepower Management Center (FMC)
- Descarga de flujo DTLS habilitada en los dispositivos afectados

Resolución

Actualice todos los dispositivos FTD/ASA afectados a una versión que incluya la corrección del

defecto ID de bug de Cisco [CSCwq32085](#).

Solución Alternativa

1. Vaya a Devices > FlexConfig en Cisco Secure Firewall Management Center.
2. Cree o edite un objeto FlexConfig.
3. Inserte el texto de la línea de comandos para deshabilitar la descarga de flujo DTLS/IPSEC para el dispositivo FTD a través de FlexConfig.

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

4. Asigne la política FlexConfig al dispositivo FTD de destino e implemente la configuración.
5. El cambio requiere un reinicio del FTD para que los cambios surtan efecto.

Causa

Los reinicios inesperados fueron causados por el ID de bug Cisco CSCwq32085 en FTD. Este defecto de software conocido puede desencadenar errores del acelerador NPU/FPGA y reinicios forzados cuando la descarga de flujo DTLS está habilitada en los appliances de las series Firepower 3100 y 4200. El defecto afecta específicamente a las funciones de aceleración de hardware y genera archivos crypto_archive con un mensaje de error de consola "KC ILK issue detected" antes de forzar los reinicios del sistema.

Contenido relacionado

- [Comprensión y solución de problemas de descarga de IPsec y DTLS en los firewalls Secure Firepower 3100 y 4200](#)

- [Configuración de objetos FlexConfig](#)
- [ID de bug de Cisco CSCwq32085](#)
- [Notas de la versión de Cisco Secure Firewall Threat Defence, versión 7.6.x](#)
- [Soporte técnico y descargas de Cisco](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).