

O Firewall Seguro Reinicializa Inesperadamente Devido a um Problema de Descarregamento de Fluxo DTLS

Contents

Problema

O Cisco Secure Firewall Threat Defense (FTD) passa por reinicializações do sistema, causando repetidamente a interrupção do serviço e sem gerar arquivos de informação de travamento tradicionais. Durante a solução de problemas, a geração repetida de arquivos `crypto_eng0_arch_*` é observada junto com o acelerador de NPU recorrente e mensagens de erro fatais FPGA que coincidem com os eventos de reinicialização.

- O diretório FTD confirma a geração repetida de arquivos `crypto_eng0_arch_*` com carimbos de data/hora que coincidem com eventos de reinicialização.

```
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
```

- Os registros de FTD mostram mensagens de erro fatais recorrentes do acelerador de NPU e do FPGA que correspondem ao tempo de reinicializações inesperadas e arquivos `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

```

- A configuração do FTD confirma que o descarregamento de fluxo DTLS está habilitado no FTD afetado, que corresponde às condições do ID de bug Cisco CSCwq32085 com defeito conhecido.

```

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

```

Ambiente

- Visto principalmente no Firepower 3100 Series, mas afeta outros modelos
- Afeta ASAs e FTDs que não estão em uma versão fixa para o problema.
- Gerenciado pelo Firepower Management Center (FMC)
- Descarregamento de fluxo DTLS habilitado nos dispositivos afetados

Resolução

Atualize todos os dispositivos FTD/ASA afetados para uma versão que inclua a correção do bug da Cisco ID [CSCwq32085](#).

Solução

1. Vá para Devices > FlexConfig no Cisco Secure Firewall Management Center.
2. Crie ou edite um Objeto FlexConfig.
3. Insira o texto da linha de comando para desativar o descarregamento de fluxo de DTLS/IPSEC para o dispositivo FTD via FlexConfig.

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

4. Atribua a Política FlexConfig ao dispositivo FTD de destino e implante a configuração.
5. A alteração requer uma reinicialização de FTD para que as alterações entrem em vigor.

Causa

As reinicializações inesperadas foram causadas pelo bug da Cisco ID CSCwq32085 no FTD. Esse defeito de software conhecido pode acionar falhas no acelerador NPU/FPGA e reinicializações forçadas quando o descarregamento de fluxo DTLS é ativado nos dispositivos Firepower 3100 e 4200 Series. O defeito afeta especificamente os recursos de aceleração de hardware e gera arquivos crypto_archive com uma mensagem de erro de console "KC ILK issue detected" antes de forçar a reinicialização do sistema.

Conteúdo relacionado

- [Entender e solucionar problemas de descarga de IPsec e DTLS no Secure Firepower 3100 e 4200](#)

- [Configurando objetos FlexConfig](#)
- [ID de bug Cisco CSCwq32085](#)
- [Notas de versão do Cisco Secure Firewall Threat Defense, versão 7.6.x](#)
- [Suporte técnico e downloads da Cisco](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.