

Identificando a versão do Catalyst 5000 EARL e outras perguntas comuns do EARL

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Convenções](#)

[O que é EARL?](#)

[Determinando a versão de EARL a partir do CLI](#)

[Determinar a versão de EARL a partir da matriz de número de peça](#)

[Supervisores do Catalyst 5000 Series do Supervisor Modular](#)

[Switches da série Catalyst 5000 de configuração fixa](#)

[Determinando a versão do EARL pelo SNMP](#)

[Por que apenas as versões 5000 do Catalyst 1 EARL são afetadas?](#)

[Se não houver redundância de STP na rede ainda assim deve ser feito uma atualização?](#)

[Catalyst 4000 e 6000 não são afetados pela vulnerabilidade 802.1x](#)

[Participação do Windows 2000 no 802.1x](#)

[Informações Relacionadas](#)

[Introduction](#)

Este documento aborda questões comuns relacionadas ao problema de vulnerabilidade 802.1x com os switches Catalyst 5000. Também está incluído neste documento como determinar a versão do Catalyst 5000 EARL. Para obter mais informações sobre a vulnerabilidade do 802.1x, consulte o seguinte aviso de segurança:

<http://www.cisco.com/warp/public/707/cisco-sa-20010413-cat5k-8021x.shtml>

[Prerequisites](#)

[Requirements](#)

Não existem requisitos específicos para este documento.

[Componentes Utilizados](#)

Este documento não se restringe a versões de software e hardware específicas.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Convenções

Consulte as [Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos](#).

O que é EARL?

O Encoded Address Recognition Logic (EARL) é um mecanismo de processamento centralizado para aprendizagem e encaminhamento de pacotes com base em endereços MAC nos Catalyst 5000 Supervisor Engines. O EARL armazena a VLAN, o endereço MAC e as relações de porta. Essas relações são usadas para a tomada de decisões de switching no hardware.

Determinando a versão de EARL a partir do CLI

Para determinar a versão de EARL na Interface de linha de comando (CLI), emita o comando `show module` a partir do Supervisor. Um exemplo segue abaixo:

```
Console (enable) sh mod
Mod Module-Name Ports Module-Type Model Serial-Num Status
-----
1 2 100BaseFX MM Supervis WS-X5506 005441962 ok
2 48 10BaseT Ethernet WS-X5012A 010308246 ok
3 48 10BaseT Ethernet WS-X5012A 010308178 ok
4 24 3 Segment 100BaseTX E WS-X5223 005389389 ok
5 12 100BaseFX MM Ethernet WS-X5201R 008951252 ok

Mod MAC-Address(es) Hw Fw Sw
-----
1 00-e0-f9-d6-64-00 to 00-e0-f9-d6-67-ff 1.0 2.2(2) 4.2(1)
2 00-90-6f-6e-75-c0 to 00-90-6f-6e-75-ef 1.0 4.2(1) 4.2(1)
3 00-90-6f-6e-5a-f0 to 00-90-6f-6e-5b-1f 1.0 4.2(1) 4.2(1)
4 00-e0-b0-fb-0a-29 to 00-e0-b0-fb-0a-2b 1.0 2.2(1) 4.2(1)
5 00-60-2f-39-3d-d4 to 00-60-2f-39-3d-df 1.1 4.1(1) 4.2(1)

Mod Sub-Type Sub-Model Sub-Serial Sub-Hw
-----
1 EARL 1+ WS-F5511 0005442554 1.0
```

O comando `show module` acima emitido a partir do Supervisor indicará a Versão do Hardware EARL no campo de Subtipo. Se o Supervisor for um EARL 1, 1.1 ou 1+,1++, o sistema será afetado pela vulnerabilidade de 802.1x. Qualquer outra versão do EARL indicada no Sub-Type (Subtipo), como NFFC, NFFC+ ou NFFC II, não é EARL 1 e não é afetada pela vulnerabilidade 802.1x.

Observação: o Supervisor IIG e IIG não imprimirão o Subtipo. O supervisor IIG e o IIG são EARL 3s e não são afetados pela vulnerabilidade de 802.1x.

Determinar a versão de EARL a partir da matriz de número de

peça

Supervisores do Catalyst 5000 Series do Supervisor Modular

Número de peça do Supervisor	Modelo de supervisor	Subtipo de versão de Earl	Tipo de sub-modelo de versão EARL	Afetado pela vulnerabilidade 802.1x
WS-X5005	Supervisor I	EARL 1	WS-F5510	Yes
WS-X5006	Supervisor I	EARL 1	WS-F5510	Yes
WS-X5009	Supervisor I	EARL 1	WS-F5510	Yes
WS-X5505	Supervisor II	EARL 1+	WS-F5511	Yes
WS-X5506	Supervisor II	EARL 1+	WS-F5511	Yes
WS-X5509	Supervisor II	EARL 1+	WS-F5511	Yes
WS-X5530-E1	Supervisor III	EARL 1++	WS-F5520	Yes
WS-X5530-E2	NFFC do Supervisor III	EARL 2 (NFFC)	WS-F5521	No
WS-X5530-E2A	NFFC-A do Supervisor III	EARL 2 (NFFC)	WS-F5521	No
WS-X5530-E3	Supervisor III NFFC II	EARL 3 (NFFC II)	WS-F5531	No
WS-X5530-E3A	Supervisor III NFFC II-A	EARL 3 (NFFC II)	WS-F5531	No
WS-X5534	Supervisor III F	EARL 1++	WS-F5520	Yes
WS-X5540	Supervisor II G	EARL 3 (NFFC II)	WS-F5531	No
WS-X5550	Supervisor III G	EARL 3 (NFFC II)	WS-F5531	No

Switches da série Catalyst 5000 de configuração fixa

Número de peça do switch	Modelo de supervisor	Subtipo de versão de Earl	Tipo de sub-modelo de versão EARL	Afetado pela vulnerabilidade de 802.1x
WS-C2901	Supervisor I	EARL 1	WS-F5510	Yes
WS-C2902	Supervisor I	EARL 1	WS-F5510	Yes
WS-C2926T	Supervisor II	EARL 1+	WS-F5511	Yes
WS-C2926G	Supervisor II	EARL 1+	WS-F5511	Yes
WS-C2926GS	Supervisor III NFFC II	EARL 3 (NFFC II)	WS-F5531	No
WS-C2926GL	Supervisor III NFFC II	EARL 3 (NFFC II)	WS-F5531	No

Observação: nas revisões anteriores do software, o EARL 3 (NFFC II) pode ser chamado de NFFC+.

[Determinando a versão do EARL pelo SNMP](#)

A versão de hardware EARL pode ser determinada pelo protocolo SNMP (Protocolo de Gerenciamento de Rede Simples). Usando

```
.iso.org.dod.internet.private.enterprises.cisco.workgroup.stack.moduleGrp.mo
```

```
duleTable.moduleEntry.moduleSubType
```

```
.1.3.6.1.4.1.9.5.1.3.1.1.16
```

Os valores de retorno podem ser:

- outro(1)
- empty(2)
- wsf5510(3) (EARL1)
- wsf5511(4) (EARL1+)
- wsx5304(6) (RSM—NÃO NO SUPERVISOR)
- wsf5520(7) (EARL1++)
- wsf5521(8) (EARL2/NFFC)
- wsf5531(9) (EARL3/NFFCII)

O Supervisor II G e IIIG não irá retornar um valor. O supervisor IIG e o IIIG são EARL 3s e não são afetados pela vulnerabilidade de 802.1x.

[Por que apenas as versões 5000 do Catalyst 1 EARL são](#)

afetadas?

As versões EARL 1 são afetadas somente porque os EARL 1 precisam ser programados para cada endereço MAC reservado individualmente. Todas as outras versões do EARL foram programadas com intervalos e, portanto, não encaminhe o quadro 802.1x.

Se não houver redundância de STP na rede ainda assim deve ser feito uma atualização?

Absolutamente, o software Catalyst 5000 ainda está encaminhando os pacotes em todas as portas. O switch deve estar descartando esses quadros de entrada. Embora a rede não sofra degradação a menos que haja redundância de STP, o switch ainda está operando incorretamente.

Catalyst 4000 e 6000 não são afetados pela vulnerabilidade 802.1x

Os switches da série Catalyst 5000 com EARL 1 são o único switch afetado. Todos os outros switches não encaminharão o quadro e, na verdade, impedirão a ocorrência de um loop STP se os switches estiverem localizados no caminho STP.

Participação do Windows 2000 no 802.1x

Atualmente, o Windows XP (Whistler) é o único sistema operacional Microsoft que suporta 802.1x. De acordo com a Microsoft, o 802.1x para Windows 2000 pode ser adicionado posteriormente por meio de uma atualização ou correção de software. Atualmente, o Windows XP (Whistler) é o único sistema operacional da Microsoft a suportar 802.1x. De acordo com a Microsoft, o 802.1x para Windows 2000 pode ser adicionado posteriormente por meio de uma atualização ou correção de software.

Informações Relacionadas

- [Notas da Versão 4.x da Família de Software Catalyst 5000](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)