Contenido

[Introducción](#)
[prerrequisitos](#)
[Requisitos](#)
[Componentes Utilizados](#)
[Convenciones](#)
[¿Qué es la EARL?](#)
[Determinación de la versión EARL desde CLI](#)
[Determine la versión de EARL en base a la matriz de números de partes](#)
[Supervisores modulares de la serie 5000 de Catalyst](#)
[Catalyst 5000 Series Switches de Configuración Fija](#)
[Determinación de la versión de EARL a través de SNMP](#)
[¿Por qué sólo las versiones de Catalyst 5000 EARL 1 están afectadas?](#)
[Si no existe redundancia de STP en la red, ¿aún así debo actualizar?](#)
[Catalyst 4000 y 6000 no son afectados por la vulnerabilidad de 802.1x](#)
[Participación de Windows 2000 en 802.1x](#)
[Información Relacionada](#)

Introducción

Este documento se ocupa de preguntas comunes que rodean el problema de vulnerabilidad 802.1x con switches Catalyst 5000. También se incluye en este documento cómo determinar la versión de EARL del Catalyst 5000. Para más información acerca de la vulnerabilidad de 802.1x, consulte la siguiente asesoría en seguridad:

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

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

¿Qué es la EARL?

La Lógica de reconocimiento de dirección codificada (EARL) es un motor de procesamiento centralizado para el aprendizaje y reenvío de paquetes basado en una dirección MAC en el Supervisor Engine de Catalyst 5000. El EARL almacena la VLAN, la dirección MAC y las relaciones entre puertos. Estas relaciones se utilizan para conmutar decisiones de hardware.

Determinación de la versión EARL desde CLI

Para determinar la versión de EARL de la interfaz de línea de comandos (CLI), ejecute el comando show module desde el supervisor. Se presenta un ejemplo a continuación:

```
Console (enable) sh modMod 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
```

El comando show module anterior ejecutado desde Supervisor indica la versión de hardware de EARL en el campo Subtipo. Si el Supervisor es un EARL 1, 1.1, o un 1+, 1++, la vulnerabilidad 802.1x afecta al sistema. Cualquier otra versión del EARL indicada en el sub-tipo como NFFC, NFFC+ o NFFC II no es EARL 1 y no resulta afectada por la vulnerabilidad 802.1x.

Nota: El Supervisor IIG y el IIIG no imprimirán el subtipo. Los supervisores IIG y IIIG son EARL 3 y no son afectados por la vulnerabilidad 802.1x.

Determine la versión de EARL en base a la matriz de números de partes

Supervisores modulares de la serie 5000 de Catalyst

Número de parte del supervisor	Modelo de Supervisor	Subtipo de la versión de EARL	Tipo de submodelo de versión EARL	Afectado por vulnerabilidad de 802.1x
WS-X5005	Supervisor I	EARL 1	WS-F5510	Sí
WS-X5006	Supervis	EARL	WS-	Sí

	or I	1	F5510	
WS-X5009	Supervisor I	EARL 1	WS-F5510	Sí
WS-X5505	Supervisor II	EARL 1+	WS-F5511	Sí
WS-X5506	Supervisor II	EARL 1+	WS-F5511	Sí
WS-X5509	Supervisor II	EARL 1+	WS-F5511	Sí
WS-X5530-E1	Supervisor III	EARL 1++	WS-F5520	Sí
WS-X5530-E2	Supervisor III NFFC	EARL 2 (NFFC)	WS-F5521	No
WS-X5530-E2A	Supervisor III NFFC-A	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	Sí
WS-X5540	Supervisor II G	EARL 3 (NFFC II)	WS-F5531	No
WS-X5550	Supervisor III G	EARL 3 (NFFC II)	WS-F5531	No

Catalyst 5000 Series Switches de Configuración Fija

Numero de parte del Switch	Modelo de Supervisor	Subtipo de la versión de EARL	Tipo de submodelo de versión EARL	Afectado por vulnerabilidad de 802.1x
WS-C2901	Supervisor I	EARL 1	WS-F5510	Sí

WS-C2902	Supervisor I	EARL 1	WS-F5510	Sí
WS-C2926T	Supervisor II	EARL 1+	WS-F5511	Sí
WS-C2926G	Supervisor II	EARL 1+	WS-F5511	Sí
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

Nota: En las revisiones del software tempranas, el CONDE 3 (el NFFC II) se puede referir como NFFC+.

Determinación de la versión de EARL a través de SNMP

La versión de hardware EARL puede determinarse con el Protocolo de administración de red simple (SNMP). Usando .iso.org.do d.internet.private.enterprises.cisco.workgroup.stack.moduleGrp.mo

“SRC_INVALID”

.1.3.6.1.4.1.9.5.1.3.1.1.16

Los valores devueltos pueden ser:

- otro(1)
- empty(2)
- wsf5510(3) (EARL1)
- wsf5511(4) (EARL1+)
- wsx5304(6) (RS--NO EN EL SUPERVISOR)
- wsf5520(7) (EARL1++)
- wsf5521(8) (EARL2/NFFC)
- wsf5531(9) (EARL3/NFFCII)

El Supervisor II G y el IIIG no devolverán un valor. Los supervisores IIG y IIIG son EARL 3 y no son afectados por la vulnerabilidad 802.1x.

¿Por qué sólo las versiones de Catalyst 5000 EARL 1 están afectadas?

Las versiones EARL1 son solamente afectadas porque los EARL1 necesitan ser programados para cada dirección MAC reservada individualmente. Todas las otras versiones de EARL se programaron con rangos y por lo tanto, no reenvían la trama 802.1x.

Si no existe redundancia de STP en la red, ¿aún así debo actualizar?

Absolutamente, el software del Catalyst 5000 todavía está remitiendo los paquetes en todos los puertos. El Switch debe caer estas tramas entrantes. Si bien la red no sufrirá ninguna degradación a menos que haya una redundancia STP, el switch aún funciona incorrectamente.

Catalyst 4000 y 6000 no son afectados por la vulnerabilidad de 802.1x

Los Catalyst 5000 Series Switch con el EARL1 son el único Switch afectado. El resto del Switches no remitirá la trama y parará realmente un STP loop de la ocurrencia si el Switches está situado en la ruta STP.

Participación de Windows 2000 en 802.1x

Actualmente, Windows XP (Whistler) es el único sistema operativo de Microsoft que admite 802.1x. Según Microsoft, el 802.1x para el Windows 2000 se pudo agregar en otro momento a través de una actualización del software o de una corrección. Actualmente, Windows XP (Whistler) es el único sistema operativo de Microsoft que admite 802.1x. Según Microsoft, el 802.1x para el Windows 2000 se pudo agregar en otro momento a través de una actualización del software o de una corrección.

Información Relacionada

- Notas de la versión 4.x del software de la familia Catalyst 5000.
- Soporte Técnico y Documentación - Cisco Systems