Como encontrar a origem de armadilhas de AuthenticationFailure de SNMP Cisco

Contents

Introduction

Este documento permite determinar o endereço IP que causou a interceptação (trap) de falha de autenticação. Uma interceptação (trap) de falha de autenticação significa que a entidade do protocolo de envio é o destinatário de uma mensagem de protocolo que não está adequadamente autenticada. Essa interceptação (trap) ocorrerá se um sistema de gerenciamento de rede (NMS) chamar o dispositivo com a string de comunidade incorreta.

Prerequisites

Requirements

Os leitores deste documento devem estar cientes destes tópicos:

- Definições de MIB
- Armadilhas do Protocolo de Gerenciamento de Rede Simples (SNMP - Simple Network Management Protocol)
- Identificadores de objeto (OIDs)

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Todas as versões do software Cisco IOS® 11.x e 12.x
- All Cisco routers and Switches
- Catalyst OS (CatOS) 6.3.1 para suporte a Cisco-System-MIB

The information in this document was created from the devices in a specific lab environment. 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.

Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Armadilhas de AuthenticationFailure

A armadilha em si não ajuda muito sem o **varbind** `authAddr` que vem com a armadilha. O **varbind** é um objeto MIB adicional que vem da MIB do sistema antigo da Cisco. O `authAddr` informa o último endereço IP de falha de autorização SNMP. Aqui estão ambas as definições de MIB:

Número de definição de MIB 1

Esta definição é de CISCOTRAP-MIB Definições:

```
.1.3.6.1.2.1.11.0.4
authenticationFailure OBJECT-TYPE
-- FROM CISCOTRAP-MIB
TRAP
VARBINDS { authAddr }
DESCRIPTION "An authenticationFailure trap signifies that the sending protocol
entity is the addressee of a protocol message that is not properly authenticated.
While implementations of the SNMP must be capable of generating this trap, they
must also be capable of suppressing the emission of such traps via an implementation-
specific mechanism."
::= { iso(1) org(3) dod(6) internet(1) mgmt(2) mib-2(1) snmp(11) snmp#(0) 4}
```

Número de definição de MIB 2

Esta definição é de OLD-CISCO-SYSTEM-MIB Definições:

```
.1.3.6.1.4.1.9.2.1.5
authAddr OBJECT-TYPE
-- FROM OLD-CISCO-SYSTEM-MIB
SYNTAX IpAddress
MAX-ACCESS read-only
STATUS Mandatory
DESCRIPTION "This variable contains the last SNMP
authorization failure IP address."
::= { ISO(1) org(3) DOD(6) Internet(1) private(4) enterprises(1) cisco(9) local(2)
  lsystem(1) 5 }
```

MIB de armadilhas gerais Cisco

Você deve carregar o MIB Cisco-General-Traps no sistema NMS para formatar corretamente a interceptação. Além disso, você deve ter todas as importações listadas na parte superior do MIB Cisco-General-Trap antes de compilar o MIB Cisco-General-Traps. Aqui está a lista:

```
IMPORTS
```

```
  sysUpTime, ifIndex, ifDescr, ifType, egpNeighAddr,
  tcpConnState
  FROM RFC1213-MIB
  cisco
  FROM CISCO-SMI
  whyReload, authAddr
  FROM OLD-CISCO-SYSTEM-MIB
  locIfReason
  FROM OLD-CISCO-INTERFACES-MIB
  tslineSesType, tsLineUser
  FROM OLD-CISCO-TS-MIB
  loctcpConnElapsed, loctcpConnInBytes, loctcpConnOutBytes
  FROM OLD-CISCO-TCP-MIB
  TRAP-TYPE
  FROM RFC-1215;
```

Após a compilação de todas as definições de MIB corretas, a armadilha se parece com isto:

```
Oct 18 16:54:04 nms-server2 snmptrapd[415]: 10.29.4.1: Authentication Failure
  Trap (0) Uptime: 148 days, 19:19:06.60,

enterprises.cisco.local.lsystem.authAddr.0 = IpAddress: 172.18.123.63

Oct 18 16:54:05 nms-server2 snmptrapd[415]: 10.29.4.1: Authentication Failure
  Trap (0) Uptime: 148 days, 19:19:07.61,

enterprises.cisco.local.lsystem.authAddr.0 = IpAddress: 172.18.123.63
```

Você pode ver que 172.18.123.63 está votando 10.29.4.1 com a string de comunidade errada. Se esse sistema for um que deve pesquisar o dispositivo 10.29.4.1, você precisa investigar 172.18.123.63 para determinar por que o sistema usa a comunidade errada. Em seguida, altere a comunidade para a string de comunidade correta . Se o sistema não for um NMS conhecido, o problema pode ser que algo está tentando invadir o dispositivo via SNMP.

Informações Relacionadas

- Notas técnicas do projeto de serviços de aplicativos IP
- Suporte Técnico e Documentação - Cisco Systems