如何查找Cisco SNMP认证失败陷井的来源

目录

简介

本文档使您能够确定导致`authenticationFailure`陷阱的IP地址。`authenticationFailure`陷阱表示发送协议实体是没有正确身份验证的协议消息的地址。如果网络管理系统(NMS)使用错误的社区字符串轮询设备，您会收到此陷阱。

先决条件

要求

本文档的读者应掌握以下这些主题的相关知识：

- MIB定义
- 简单网络管理协议(SNMP)陷阱
- 对象标识符(OID)

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 所有Cisco IOS®软件版本11.x和12.x
- 所有思科路由器和交换机
- Catalyst OS(CatOS)6.3.1，用于Cisco-System-MIB支持

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文件规则的更多信息请参见“ Cisco技术提示规则”。

身份验证失败陷阱

没有陷阱附带的**varbind** `authAddr` ，陷阱本身就没有太大帮助。**varbind**是来自旧Cisco-System MIB的附加MIB对象。`authAddr` 将告知您最后一个SNMP授权失败IP地址。以下是两个MIB定义：

MIB定义编号1

此定义来自CISCOTRAP-MIB定义:

```
.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}
```

MIB定义编号2

此定义来自OLD-CISCO-SYSTEM-MIB定义:

```
.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 }
```

Cisco-General-Traps MIB

您必须在NMS系统中加载Cisco-General-Traps MIB，才能正确格式化陷阱。此外，在编译Cisco-General-Traps MIB之前，必须将所有导入列在Cisco-General-Trap MIB的顶部。以下是列表：

```
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;
```

编译所有正确的MIB定义后，陷阱如下所示：

```
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
```

您可以看到172.18.123.63是轮询10.29.4.1的社区字符串错误。如果此系统应轮询10.29.4.1设备，则您需要调查172.18.123.63，以确定系统使用错误社区的原因。然后，将社区更改为正确的社区字符串。如果系统不是已知的NMS，则问题可能是有人尝试通过SNMP侵入设备。

相关信息

- IP应用服务设计技术说明
- 技术支持和文档 - Cisco Systems