# 解决在使用IPv6 ACL时的完整IPv6数据包丢弃

## 目录



## 简介

本文档介绍ACE中带有全零前缀的IPv6 ACL可以匹配所有IPv6数据包及其解决方法。

## 先决条件

### 要求

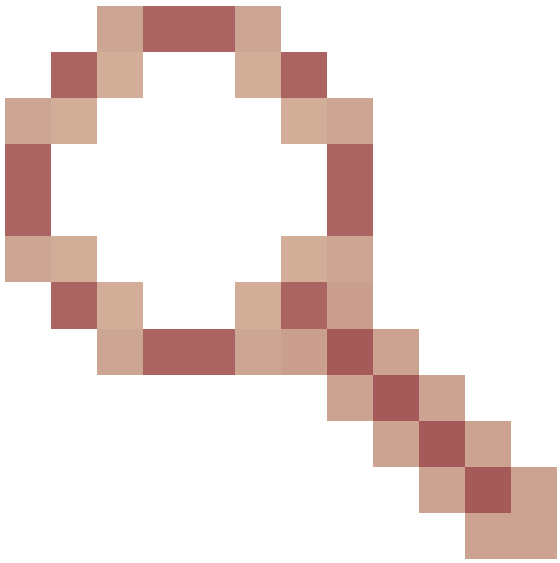
Cisco 建议您了解以下主题：

- 思科IOS® XR路由器上的IPv6 ACL（访问控制列表）配置
- Cisco IOS® XR路由器上的ACL硬件编程

### 使用的组件

本文档中的信息基于以下软件和硬件版本：

- IPv6 ACL应用压缩级别2或3



- 思科IOS® XR版本，不修正思科漏洞ID CSCwe08250

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。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

# 背景信息

在RFC(请求注解)4291中，IPv6地址：：/128是为未指定地址保留。它绝不能分配给任何节点，因此最佳做法是在IPv6 Bogon过滤中拒绝此地址。

# 问题

包含：：/128的ACE（访问控制条目）的IPv6 ACL可以匹配其应用到的接口上的任何IPv6数据包。

下面是实验中此观察的示例。

使用：：/128分别与IPv6源地址和目标地址配置IPv6 ACL：

```
ipv6 access-list PREFIX_ALL_ZERO
 10 remark ** HOST MASK **
 11 deny ipv6 any host :: log
 12 deny ipv6 host :: any log
```

将PING(数据包互联网或网络间探测器)流量发送到非零IPv6目标地址：

```
RP/0/RP0/CPU0:router#ping fd00:4860:1:1::150 count 100 timeout 0
Thu Sep 14 12:30:23.412 UTC
pings with timeout=0 may result in system instability and
control protocol flaps resulting in traffic impact.
Do you really want to continue[confirm with only 'y' or 'n'] [y/n] :y
Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to FD00:4860:1:1::150, timeout is 0 seconds:
....................................................................................................
Success rate is 0 percent (0/100)
```

ACE11丢弃了数据包：

RP/0/RP0/CPU0:router#show access-lists ipv6 PREFIX_ALL_ZERO hardware ingress lo
Thu Sep 14 12:30:46.346 UTC
ipv6 access-list PREFIX_ALL_ZERO
11 deny ipv6 any host :: log (100 matches)
12 deny ipv6 host :: any log

删除ACE 11时，丢弃会移至ACE 12：

RP/0/RP0/CPU0:router#clear access-list ipv6 PREFIX_ALL_ZERO hardware ingress location 0/RP0/CPU0

Thu Sep 14 12:31:34.899 UTC

RP/0/RP0/CPU0:router#ping fd00:4860:1:1::150 count 100 timeout 0

Thu Sep 14 12:31:39.482 UTC

pings with timeout=0 may result in system instability and

control protocol flaps resulting in traffic impact.

Do you really want to continue[confirm with only 'y' or 'n'] [y/n] :y

Type escape sequence to abort.

Sending 100, 100-byte ICMP Echos to FD00:4860:1:1::150, timeout is 0 seconds:

.....

Success rate is 0 percent (0/100)

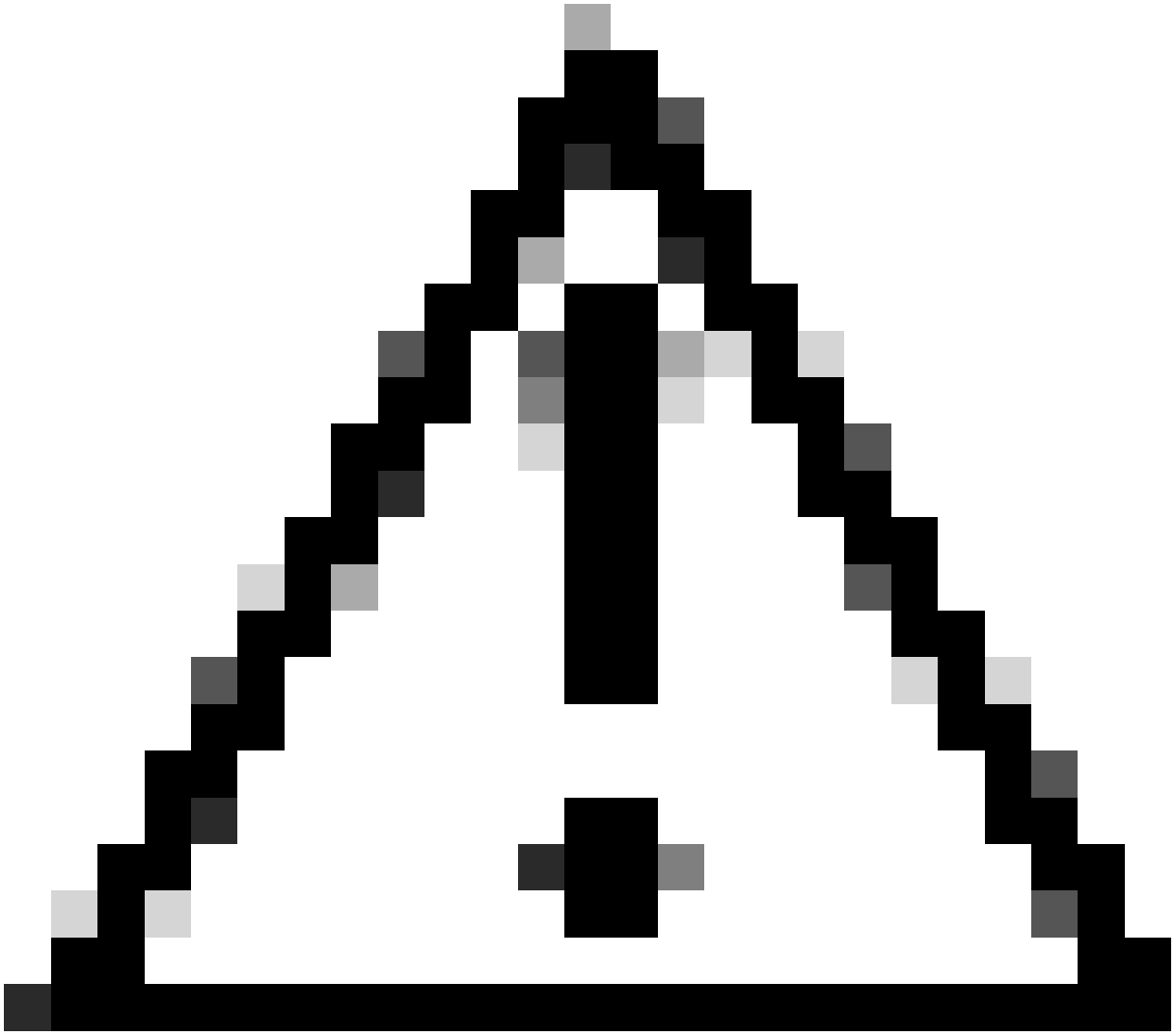
RP/0/RP0/CPU0:router#show access-lists ipv6 PREFIX_ALL_ZERO hardware ingress location 0/RP0/CPU0

Thu Sep 14 12:31:45.229 UTC

ipv6 access-list PREFIX_ALL_ZERO

12 deny ipv6 host :: any log (100 matches)

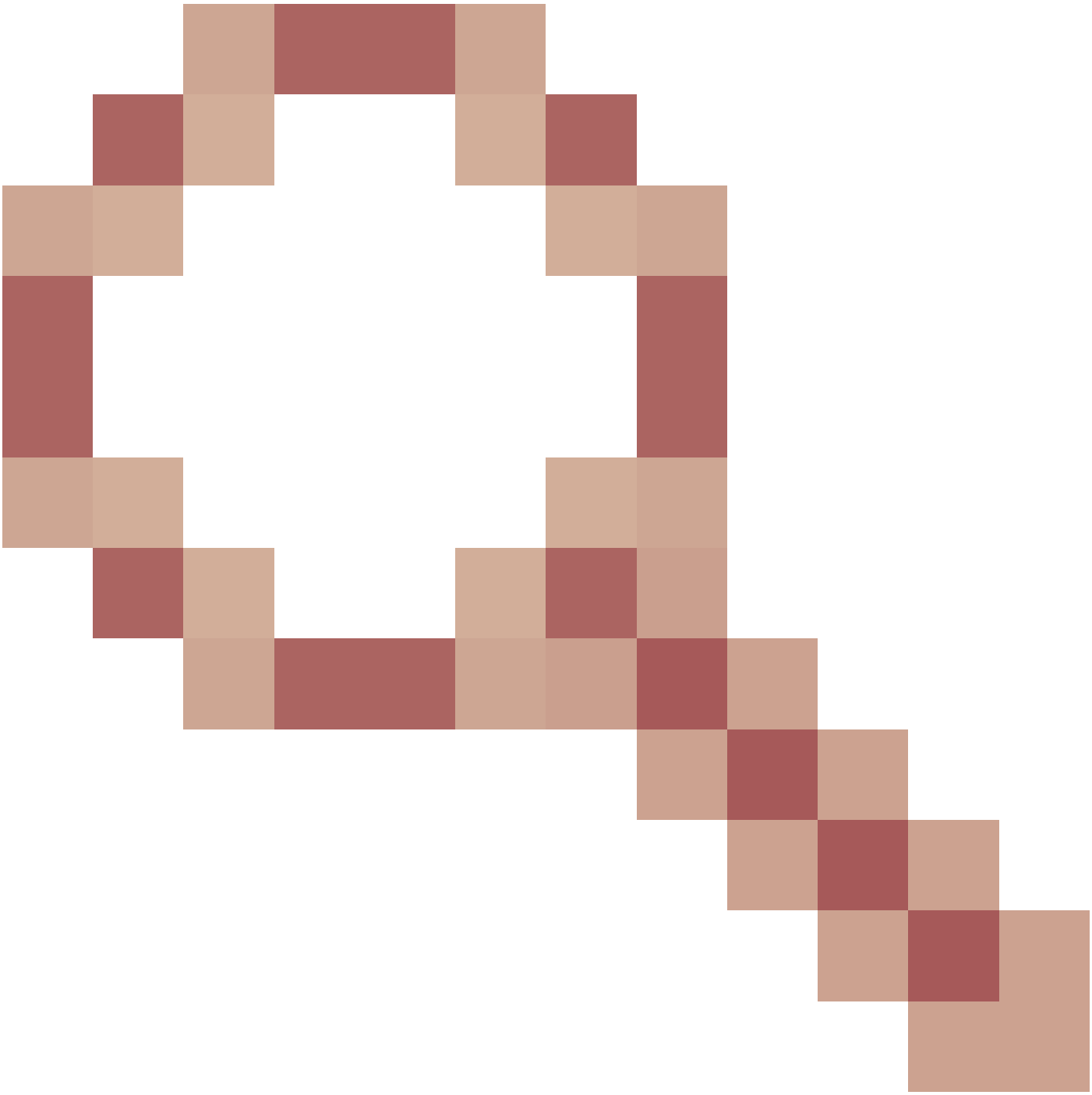
这些ACE应该只丢弃源地址或目标地址全部为零的数据包。
但是，所有流量（即使源或目标并非全部为零）都将被丢弃。



注意：此不匹配行为适用于ACE上从/1到/128的IPv6子网标记长度，而不只是示例中的/128。

## 解决方案

修正了Cisco Bug ID CSCwe08250的Cisco IOS® XR版本可以



更正这一错误行为。

在运行没有此修复程序的Cisco IOS® XR路由器上，存在以下解决方法：

- 使用混合ACL并将：：/<x>从ACL移动到网络对象组，以匹配全部为零的源或目标地址。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。