 在最近发表的一个IOS安全公告里，Cisco警告称在Internet上使用的一个公共管理协议可以被利用来发动针对Cisco 路由器或其他基于IP的设备的拒绝服务攻击。 该安全公告对基于Internet控制报文协议（ICMP）的潜在攻击发出了警告，攻击可能导致基于IOS的设备不可访问。思科的安全公告是根据英国国家基础设施安全协调中心（NISCC）发布的一份通报提出的，而NISCC发布的通报则是参考了IETF网站发表的一份描写ICMP如何被用于发起针对TCP通信的DoS攻击的文档。 ICMP是TCP/IP协议族的一个子协议，用于在IP主机、路由器之间传递控制消息。控制消息是指网络通不通、主机是否可达、路由是否可用等网络本身的消息。据IETF文档说，攻击者有可能给运行TCP的设备发送某些ICMP“ 硬件错误 ”消息，导致设备重置TCP连接或降低TCP连接的吞吐率。如果反复发送这样的ICMP消息，设备就可能变得对网络不可访问。IETF文档还概述了利用路径最大传输单元发现（PMTUD）的另一种DoS攻击方法。PMTUD是ICMP的一个处理错误消息的机制。 Cisco表示，只有运行启用了PMTUD的IOS的路由器和其他设备才会受到这种攻击。它指出ICMP“ 硬件错误 ”消息攻击对思科设备无效。不过，所有版本的IOS（10.x、11.x和12.x）易受基于PMTUD的攻击。其他不基于IOS的设备也易受攻击，包括思科Aironet WLAN设备、堆叠式和机架式Catalyst交换机和ONS光网络设备。 Cisco表示，在运行IPv4的IOS设备

中PMTUD默认是禁用的，但在运行IPv6或IPSec的IOS设备中PMTUD默认是启用的，如VPN设备和PIX安全应用设备。Cisco警告说，他的基于IOS-XR操作系统的CRS-1互联网路由器是易受PMTUD攻击和ICMP“硬错误”消息攻击。（PMTUD在IOS-XR中默认是禁用的）。Cisco已经针对这些漏洞发布了软件补丁程序。同时，Cisco表示在Cisco设备中禁用PMTUD也是解决问题的一个办法。