思科推新安全建议DoS攻击成幕后推手思科认证 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/644/2021_2022__E6_80_9D_E7_A7_91_E6_8E_A8_E6_c101_644275.htm 早些时候，思科为其Internetwork Operating System(IOS)推出了九项建议，该操作系统软件适用于大多数企业路由和交换机。思科公司还为思科统一通讯管理程序提供了两项建议。 思科的补丁周期以半年为期，这些建议正是补丁更新的一部分。总体而言，上面提到的11项建议涵盖了12个潜在漏洞。这些建议提到，有八个地址漏洞可能使用户遭受DoS攻击。 在DoS攻击中，入侵者会用一些请求某类服务的数据包淹没服务器或是其他网络设备。分布式拒绝服务(DDOS)由多台电脑发出的大量虚假请求组成，二者都是为了避开被察觉的同时增加攻击强度。 根据这些建议所描述，攻击者会用H.323多媒体协议数据包，网络时间协议数据包，会话发起协议数据包等制造DoS攻击，这些攻击可能导致思科路由或交换机瘫痪。 这些建议暗示严格限制协议数据包的类型可以减缓此类攻击。思科为H.323漏洞采取的权宜之计是，一旦网络装载的数据不使用规定的协议，那么就禁用该服务。事实上，针对这些漏洞推出的补丁可以禁用这些协议。尽管如此，使用这些服务的人或许还是要寻求其他方法来防御此类攻击。 在保留下来的补丁中，其中有两个在验证控件方面存在缺陷，另外一个可以处理那些消耗设备安全密钥的攻击。对于这类问题，思科也已经推出了补丁。 从2008年3月开始，思科就一直致力于推出非紧急的安全漏洞补丁以及半年更新一次的IOS安全建议。该公司将在2010年3月推出下一轮安全补丁。 编辑特别推荐: 关于思科

认证考试的注意事项 Cisco认证总结CCNA重难点 思科认证考试形式介绍 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com