

安全协议出漏洞书室思科、Juniper受牵连 PDF转换可能丢失图片或格式，建议阅读原文

https://www.100test.com/kao_ti2020/142/2021_2022__E5_AE_89_E5_85_A8_E5_8D_8F_E8_c101_142047.htm 当地时间本周一，芬兰奥卢大学的研究人员宣布，他们发现了互联网安全关联和密钥管理协议（ISAKMP）中的一个缺陷。该技术被应用在了IPsec虚拟专用网络和来自思科、Juniper等网络巨头的防火墙产品。据英国国家基础设施安全协调中心（NISCC）和芬兰CERT联合发表的一份公告称，这一问题的严重性根据不同软件厂商而有所不同。公告说，这些缺陷可能导致拒绝服务攻击、格式字符串攻击、缓冲区溢出缺陷攻击。所有这些攻击可能会关闭设备，或放慢互联网上的数据传输速度。NISCC警告说，它们还可能使黑客执行代码和挟持设备。ISAKMP为其它安全协议提供关联服务，用于建立通过公共互联网的安全连接，它是IPsec中的一个重要部分。拥有分公司的大公司利用IPsec使分公司安全地访问总公司的系统，远程员工也可以利用该技术访问他们公司的内部网络。思科和Juniper这二大网络巨头承认它们的一些产品可能会受到攻击。思科表示，这一缺陷可导致设备反复重启，造成临时性的拒绝服务攻击。但它没有提及设备被黑客控制的可能性。思科已经发布了修正这一问题的补丁软件，并发布了安全公告。受影响的产品包括Cisco IOS、Cisco PIX Firewall、Cisco Firewall Services Module、Cisco VPN 3000 Series Concentrators、Cisco MDS Series SanOS。受影响的Juniper产品包括M系列、T系列、J系列、E系列路由器，以及大多数版本的Junos、JunoSe安全软件。该公司的一名代表说，Juniper在6月份就

知道了这一问题，因此在7月28日之后发布的软件都解决了这一问题。Openswan项目也受到了影响。它也发布了Openswan 2.4.2，修正了该问题。3Com表示，它正在研究这一问题，看其产品是否受到了影响。微软和IBM则表示，它们的产品没有受到影响。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