思科惊现严重漏洞影响骨干网络 PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/251/2021_2022__E6_80_9D_E7_A7_91_E6_83_8A_E7_c101_251145.htm 国家计算机网络应急技术处理协调中心(CNCERT)日前发布安全公告称，思科系统中存在三个安全漏洞，此漏洞影响所有运行IOS的思科设备。这是继2004年4月思科TCP漏洞之后，三年来CNCERT第一次发布思科设备漏洞。CNCERT近三年所有公告，涉及以微软居多，思科仅此两次。 目前尚不清楚此漏洞是否造成损失。不过专家指出：“ 由于我国电信、网通、移动、联通、铁通等五大基础运营商核心路由器均使用思科产品，因此漏洞对我国的骨干网安全存在潜在威胁。为保障公共互联网安全，请相关用户及时修补漏洞。 ”根据安全公告，漏洞包括Cisco IOS TCP包处理漏洞、Cisco IOS IPv4伪造包漏洞、Cisco IOS IPv6伪造包漏洞。远程攻击者可以利用IOS中的漏洞让受影响的设备重载操作系统。在重载期间，由于数据包不能被正确处理，实际相当于拒绝服务攻击，持续利用漏洞会造成持续的拒绝服务攻击。 据了解，思科已经提供了修复全部漏洞的软件，可从其官方网站下载。互联网技术专家指出，用户只要及时下载、安装补丁，将可避免遭受安全威胁。 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