



MSR系列漏洞解决方法

攻击防范及检测

软件相关

zhiliao_LxX7nl

2023-09-13 发表

问题描述

MSR1000系列、MSR26系列、MSR36系列、MSR56系列、MSR810、MSR830、MSR610漏洞解决方法

解决方法

可以在下面的链接进行查看漏洞说明，可以根据漏洞编码看是否涉及
知识库 - 知了社区 (h3c.com)

处理方法可以在知了社区进行搜索对应的漏洞编码，如果有的漏洞搜索不到可以联系下400

The screenshot shows the search results for CVE-2011-1473 on the H3C Knowledge Base website. The search bar at the top contains the text 'CVE-2011-1473'. Below the search bar, there are several search results listed:

- MSR路由器 CVE-2011-1473漏洞处理方法**
· 我司中低端路由器设备容易被第三方安全设备扫描出以下两个漏洞：服务器支持 TLS Client-initiated 重协商攻击(CVE-2011-1473) SSL/TLS 服务器端时 Diffie-Hellman 公共密钥交换 第二个漏洞可参考防火墙漏洞处理：<https://zhiliao.h3c.com/Theme/details/192779> 第一个漏洞中最大的问题是安全设备发现我网443端口始终开放，我网中低端路由器开放80/443端口除了用于http/https 网页浏览外，还可用于自...
林宇阳 2022-03-09创建 337
- Primera 存储针对 CVE-2011-1473 漏洞扫描问题**
· 某运营商通过漏洞扫描，发现Primera存在 CVE-2011-1473 漏洞问题，希望我司解决，该漏洞描述：** DISPUTED ** OpenSSL before 0.9.8i, and 0.9.8m through 1.x, does not properly restrict client-initiated renegotiation within the SSL and TLS protocols, which might make it easier for remote attac...
孔耀【技术大咖】 2022-05-18创建 1438
- H3C自研服务器HDM被绿盟软件扫描发现安全漏洞--CVE-2017-15906、CVE-2018-15919、CVE-2011-1473及SSH 服务支持弱加密算法**
· H3C自研服务器 绿盟软件漏洞扫描发现OpenSSH和 OpenSSL的若干中危漏洞： 1. OpenSSH 安全漏洞 CVE-2017-15906； 2. OpenSSH 用户收发消息 CVE-2018-15919； 3. SSH 服务器支持弱加密算法 4. 服务器支持 TLS Client-initiated 重协商攻击 CVE-2011-1473。 定位是HDM的漏洞，查阅HDM的相关手册。 ***** 1) 【CVE-2017-15906 漏洞】 OpenSSH 7.6之前的版本中的tftp-s...
王怀志 2021-07-13创建 112
- 服务器支持 TLS Client-initiated 重协商攻击(CVE-2011-1473)**
· 由于服务器端的重协商协商的开启是客户端的15倍，则攻击者可利用这个过程向服务器端发起拒绝服务攻击，OpenSSL 1.0.2及以前版本受影响 升级R9616P39或R9628P2412或更新
曹旻 2021-06-18创建 2857
- License Server涉及服务器支持 TLS Client-initiated 重协商攻击(CVE-2011-1473)**
· 该漏洞存在于SSL renegotiation的过程中，对于使用SSL重协商功能的服务器都会受到影响。特别的， renegotiation被用于浏览器到服务器之间的验证。虽然目前可以在不启用renegotiation进程的情况下使用HTTPS，但很多服务器的默认设置均启用了renegotiation功能。该漏洞只需要一台普通电脑和SSL连接即可轻松攻破SSL服务器，而对于大型服务器集群中，则需要20台电脑和120Kbps的网络连接即可实现。SSL是银行、网上电子邮件服务和其他用于服务器和用户之间保护私人...
田钰磊 2021-07-24创建 964

