S5130-HI 交换机SSH和NTP相关漏洞说明及解决办法

NTP SSH 孙兆强 2018-06-28 发表

组网及说明

无

问题描述

无

过程分析

无

解决方法

70658-启用 SSH 服务器 CBC 模式密码	SSH 服务器被配置为使用密码块链接。 SSH 服务器被配置为支持密码块链 (CBC) 加密。这可能允许攻击者从密文中恢复明文消息。 请注意, 此插件仅检查 SSH 服务器的选项, 并且不检查易受攻击的软件版本。	2（Low）	请与供应商联系或查阅产品文档, 以禁用 CBC 模式密码加密, 并启用点击率或 GCM 密码模式加密。	不涉及
71049-启用SSH弱MAC算法	远程 SSH 服务器被配置为允许 MD5 和96位 MAC 算法。 远程 SSH 服务器被配置为允许 MD5 或96位 MAC 算法, 两者都被认为是弱的。 请注意, 此插件只检查 SSH 服务器的选项, 并且不检查易受攻击的软件版本。	2（Low）	请与供应商联系或查阅产品文档, 以禁用 MD5 和 96位 MAC 算法。	可以用ssh2 algorithm 屏蔽掉MD5-96
97861-网络时间协议 (NTP) 模式6扫描仪	远程 NTP 服务器响应模式6查询。 远程 NTP 服务器响应模式6查询。响应这些查询的设备有可能在 NTP 放大攻击中使用。未经身份验证的远程攻击者可能通过巧尽心思构建的模式6查询来利用此漏洞, 从而导致反映拒绝服务条件。	3（Medium）	限制 NTP 模式6查询。	CVE-2015-7855 涉及，新版本已经修复
10882-SSH 协议版本1会话密钥检索	远程服务提供了不安全的加密协议。 远程 ssh 守护进程支持使用 SSH 协议的版本1.33 和/或 1.5 进行的连接。 这些协议不是完全加密的安全的, 所以不应该使用它们。	4（High）	禁用与协议1版的兼容性。	默认不涉及