防火墙是否涉及TLS 版本 1.0 协议检测漏洞

漏洞相关 **王奎银** 2022-02-23 发表

漏洞相关信息

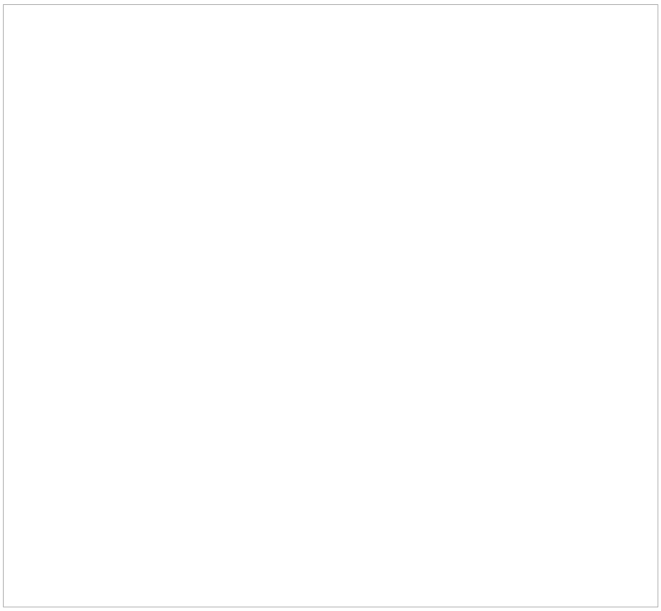
漏洞编号： 无
漏洞名称： TLS 版本 1.0 协议检测
产品型号及版本： 防火墙、负载均衡、入侵防御

漏洞描述

远程服务接受使用 TLS 1.0 加密的连接。TLS 1.0 有许多加密设计缺陷。TLS 1.0的现代实现缓解了这些问题，但较新版本的TLS（如1.2和1.3）是针对这些缺陷而设计的，应尽可能使用。自 2020 年 3 月 31 日起，为 TLS 1.2 及更高版本启用了鈥樋的端点将不再在 major Web 浏览器和主要供应商中正常运行。PCI DSS v3.2 要求在 2018 年 6 月 30 日之前完全禁用 TLS 1.0，但 POS POI 终端（以及它们所连接的 SSL/TLS 终止点）除外，这些终端可以验证为不容易受到任何已知 exploit 的影响。

漏洞解决方案

创建ssl服务器端策略，关闭tls1.0和ssl3.0.



```
[M9006_IRF]dis ssl server-policy test
 SSL server policy: test
     Version-info:
         SSL3.0: Enabled
         TLS1.0: Disabled
         TLS1.1: Enabled
         TLS1.2: Enabled
     PKI domain:
     Ciphersuites:
         RSA_AES_128_CBC_SHA
         RSA_DES_CBC_SHA
         RSA_RC4_128_MD5
         RSA_RC4_128_SHA
         RSA_3DES_CBC_SHA
         RSA_AES_256_CBC_SHA
         EXP_RSA_RC4_MD5
         RSA_RC2_CBC_MD5
         EXP_RSA_DES_CBC_SHA
         DHE_RSA_AES_128_CBC_SHA
         DHE_RSA_AES_256_CBC_SHA
         RSA_AES_128_CBC_SHA256
         RSA_AES_256_CBC_SHA256
         DHE_RSA_AES_128_CBC_SHA256
         DHE_RSA_AES_256_CBC_SHA256
[M9006_IRF]ssl
[M9006_IRF]ssl ser
[M9006_IRF]ssl server-policy test
[M9006_IRF-ssl-server-policy-test]dis th
#
ssl server-policy test
 version tls1.0 disable
#
return
[M9006_IRF-ssl-server-policy-test]
```

禁用当前对外提供的https/http服务

[H3C] undo ip https enable

[H3C] undo ip http enable

配置SSL服务如HTTPS服务引用前面自定义的SSL Server端策略：

[H3C] ip https ssl-server-policy test

重新使能https/http服务

[H3C] ip https enable

[H3C] ip http enable

如果有需要调整算法，可以参考这个的漏洞进行算法调整

防火墙、IPS和LB产品是否涉及(CVE-2015-2808) SSL/TLS 受诫礼(BAR-MITZVAH)攻击漏洞【原理扫描】 - 知了社区 (h3c.com)