SSL版本2和3协议检测

漏洞相关 **王奎银** 2022-01-07 发表

漏洞相关信息

漏洞编号： 无
漏洞名称： SSL版本2和3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

SSL3.0是已过时且不安全的协议，目前已被TLS 1.0，TLS 1.1，TLS 1.2替代，因为兼容性原因，大多数的TLS实现依然兼容SSL3.0。
为了通用性的考虑，目前多数浏览器版本都支持SSL3.0，TLS协议的握手阶段包含了版本协商步骤，一般来说，客户端和服务器端的最新的协议版本将会被使用。其在与服务器端的握手阶段进行版本协商的时候，首先提供其所支持协议的最新版本，若该握手失败，则尝试以较旧的协议版本协商。能够实施中间人攻击的攻击者通过使受影响版本浏览器与服务器端使用较新协议的协商的连接失败，可以成功实现降级攻击，从而使得客户端与服务器端使用不安全的SSL3.0进行通信，此时，由于SSL 3.0使用的CBC块加密的实现存在漏洞，攻击者可以成功破解SSL连接的加密信息，比如获取用户COOKIE数据。这种攻击被称为POODLE攻击(Padding Oracle On Downgraded Legacy Encryption)。
此漏洞影响绝大多数SSL服务器和客户端，影响范围广泛。但攻击者如要利用成功，需要能够控制客户端和服务器之间的数据(执行中间人攻击)。

漏洞解决方案

防火墙等不支持ssl2.0，不涉及ssl2.0
iware平台存在此漏洞，建议关闭https登录使用http登录，或者在设备web管理口下面的访问控制列表中只放行某个管理网段的地址，排除掉漏扫的地址，功能效果类似于V7的ip https acl X.X.X.X。

Comware平台可以关闭ssl3.0并重启https服务：
[H3C]ssl version ssl3.0 disable
[H3C]undo ip http enable
[H3C]undo ip https enable
[H3C]ip http enable
[H3C]ip https enable
需要说明的是，如果启用了SSLVPN功能，需要在分别在sslvpn gateway和sslvpn context下重启服务：
[H3C -sslvpn-gateway-gw]undo service enable
[H3C -sslvpn-gateway-gw]service enable
[H3C -sslvpn-context-test]undo service enable
[H3C -sslvpn-context-test]service enable