ASA BEAST漏洞解决方案

目录

简介

本文档介绍思科自适应安全设备(ASA)软件中允许未授权用户访问受保护内容的漏洞。此外，还介绍了此问题的解决方法。

问题

攻击者利用浏览器攻击SSL/TLS(BEAST)漏洞，以便通过密码块链(CBC)加密模式中的初始化矢量(IV)链，以已知明文攻击，有效读取受保护的内容。

攻击使用的工具利用广泛使用的传输层安全版本1(TLSv1)协议中的漏洞。问题不在于协议本身，而在于它使用的密码套件。TLSv1和安全套接字层第3版(SSLv3)支持CBC密码，Padding Oracle攻击发生在此处。

用户影响

正如“可信互联网移动”所创建的SSL Pulse SSL实施调查所显示，超过75%的SSL服务器容易受此漏洞的影响。然而，BEAST工具涉及的物流相当复杂。为了使用BEAST窃听流量，攻击者必须能够非常快速地读取和插入数据包。这可能会限制BEAST攻击的有效目标。例如，BEAST攻击者可以有效地在WIFI热点或所有Internet流量在此通过有限数量的网络网关瓶颈捕获随机流量。

解决方案

BEAST是对协议使用的密码中的弱点的利用。由于它影响CBC密码，因此此问题的原始解决方法是切换到RC4密码。然而，2013年发表的《RC4密钥调度算法的缺点》一文揭示出，即使是RC4，也存在其不适宜的缺点。

为解决此问题，思科为ASA实施了以下两项修复：

- Cisco Bug ID CSCts83720:*升级到TLS 1.1/1.2*

升级并使用TLS 1.1/1.2。此解决方案的限制是它仅适用于ASA 5500-X ASA平台。传统ASA平台（ASA 5505和ASA 5500系列）上的加密硬件不支持TLSv1.2。因此，针对这些平台进行修复是不可行的。

由于协议限制，SSLv3或TLSv1.0没有解决方案；但是，大多数现代浏览器都采用了不同的缓解方式。

- 思科漏洞ID CSCuc85781:*WebVPN Cookie随机化*

对于不支持TLSv1.2的ASA软件版本，思科使用此修复将cookie随机化以降低风险。这并不能完全阻止BEAST攻击，但有助于缓解攻击。

提示：要完全防范BEAST漏洞，唯一的方法是使用TLSv1.2。这与密码类似。思科继续在较新的代码中添加更新、更强大的密码，而较旧的密码可能存在已知问题（例如RC4）。 因此，思科建议您使用较新的协议和密码。