HTTP安全返回头Strict-Transport-Security

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： HTTP安全返回头Strict-Transport-Security

产品型号及版本： 防火墙、负载均衡、入侵防御

漏洞描述

HTTP协议本身是明文，这意味着可以捕获通过HTTP传输的任何数据并查看内容。 为了保护数据的私密性并防止数据被截获，HTTP通常通过安全套接字层（SSL）或传输层安全性（TLS）连接进行隧道传输。 当使用这些加密标准中的任何一个时，它被称为HTTPS。 HTTP严格传输安全性（HSTS）是可选的响应头，可以在服务器上配置，以指示浏览器仅通过HTTPS进行通信。即使用户在同一台服务器上请求HTTP资源，浏览器也会执行此操作。网络犯罪分子通常会试图利用HTTP攻击从客户端传送到服务器的敏感信息。 这可以通过各种中间人（MiTM）攻击或网络数据包捕获进行。扫描器发现受影响的应用程序正在使用HTTPS，但不使用HSTS标头。

【原理介绍】

Strict-Transport-Security响应头是要求客户端（即PC浏览器）禁用HTTP协议。尝试后续都通过HTTPS协议进行通信。

由于HTTPS协议存在加密层，本身更安全，故该响应头也是为了安全考虑，希望服务端能返回。

【扫漏原理】

扫漏软件应该只检测HTTP响应报文中是否存在Strict-Transport-Security该响应报文，并不关心设备侧具体配置。所以报了这个漏洞

漏洞解决方案

【规避措施】

从该报文实现原理上可以有如下解释：

由于现场设备本身不开启HTTP，只开启HTTPS。本身已经可以确保所有请求通过HTTPS协议进行传输。所以该报文头即使不返回，也不会有安全隐患。

我司防火墙不涉及该漏洞。