SecCenter CSAP-ESM-AV 终端杀毒（纯杀毒功能）是否涉及SSL/TIS 受诚礼(BAR-MITZVAH)攻击漏洞(CVE-2015-2808)

漏洞扫描 卢鹏 2024-04-23 发表

漏洞相关信息

漏洞编号： SSL/TIS 受诚礼(BAR-MITZVAH)攻击漏洞

漏洞名称： CVE-2015-2808

产品型号及版本： SecCenter CSAP-ESM-AV 终端杀毒（纯杀毒功能）

漏洞描述

SSL/TLS受诚礼（BAR-MITZVAH）攻击漏洞（CVE-2015-2808

SSL/TLS协议是一个被广泛使用的加密协议,Bar Mitzvah攻击实际上是利用了"不变性漏洞"，这是RC4算法中的一个缺陷，它能够在某些情况下泄露SSL/TLS加密流量中的密文，从而将账户用户名密码，信用卡数据和其他敏感信息泄露给黑客。

在V7平台的设备不仅仅是无线控制器开启了HTTPS的web服务，其中就默认支持了RC4的算法，虽然当前主流的新版浏览器都已经正式不支持RC4算法，但是因为设备本身默认开启，对安全敏感性要求较高的用户会提出这方面的要求。

漏洞解决方案

不涉及