ACG1000-EE 设备SSL/TLS 受诫礼(BAR-MITZVAH)攻击漏洞(CVE-2015-2808)漏洞

ACG1000 漏洞相关 **吴超** 2021-05-18 发表

漏洞相关信息

漏洞编号： CVE-2015-2808

漏洞名称： SSL/TLS 受诫礼(BAR-MITZVAH)攻击漏洞

产品型号及版本： ACG1000-EE 6609P06

漏洞描述

RC4加密算法是密钥长度可变的流加密算法簇，由Ron Rivest在1987年设计的。

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。

参考信息：

http://cr.yp.to/talks/2013.03.12/slides.pdf

http://www.isg.rhul.ac.uk/tls/

http://www.freebuf.com/articles/network/62442.html

漏洞解决方案

升级ACG1000软件版本至6611P12版本可以解决