ADWAN5.0承载网方案相关产品不涉及NicheStack TCP/IP 堆栈多个高危漏洞

ADWAN控制器 ADWAN解决方案 田航磊 2021-08-14 发表

漏洞描述

漏洞描述：

（1）CVE-2020-25928：解析DNS 响应时发生越界读/写，导致远程代码执行。

（2）CVE-2021-31226：解析HTTPpost 请求时的堆缓冲区溢出漏洞，可导致远程代码执行。

（3）CVE-2020-25927：解析DNS 响应时越界读取，可导致拒绝服务。

（4）CVE-2020-25767：解析DNS 域名时越界读取，可导致拒绝服务和信息泄露。

（5）CVE-2021-31227：解析HTTPpost 请求时的堆缓冲区溢出漏洞，可导致拒绝服务。

（6）CVE-2021-31400：TCP 带外紧急数据处理功能中存在无限循环情况，导致拒绝服务。

（7）CVE-2021-31401：TCP 头部处理代码中的整数溢出漏洞。

（8）CVE-2020-35683：解析ICMP 数据包时越界读取，导致拒绝服务。

（9）CVE-2020-35684：解析TCP 数据包时越界读取，导致拒绝服务。

（10）CVE-2020-35685：TCP 连接中可预测的初始序列号(ISN)，导致TCP 欺骗。

（11）CVE-2021-27565：收到未知HTTP 请求时出现拒绝服务情况。

（12）CVE-2021-36762：TFTP 数据包处理功能中的越界读取，导致拒绝服务。

（13）CVE-2020-25926：DNS 客户端没有设置足够随机的事务ID，导致缓存中毒。

（14）CVE-2021-31228：可以预测DNS 查询的源端口发送伪造的DNS 响应包，导致缓存中毒。

受影响版本：

NicheStack < 4.3

漏洞解决方案

SNA Center、SeerEngine-WAN、SeerAnalyzer、License Server产品不涉及NicheStack TCP/IP堆栈多个高危漏洞。