ADWAN5.0承载网方案相关产品不涉及Webmin文件管理器模块权限提升漏洞

ADWAN解决方案 ADWAN控制器 田航磊 2022-03-14 发表

漏洞相关信息

漏洞编号： CVE-2022-0824、CVE-2022-0829

漏洞名称： Webmin文件管理器模块权限提升漏洞

产品型号及版本： SNA Center E1211、SeerEngine-WAN E6105H12、SeerAnalyzer E2101P10、License Server E1153

漏洞描述

一、漏洞描述

1、CVE-2022-0824是Webmin版本1.984及更低版本的文件管理器中存在能够造成特权提升的漏洞。如果使用默认的 Authentic 主题，没有配置任何文件管理器模块限制的低特权 Webmin 用户可以远程下载 .cgi 文件，修改 .cgi 文件权限，通过在文件管理器中链接这些功能，可以通过精心制作的 .cgi 文件实现远程代码执行。

2、CVE-2022-0829是任何经过身份验证的低权限用户都可以访问该/cron/save_allow.cgi端点，从而控制用户对 cron 作业的访问。他们可以允许和拒绝其他用户访问影响 Scheduled Cron Jobs 模块的 cron 作业。

二、受影响版本

Webmin <= 1.984

漏洞解决方案

SNA Center、SeerEngine-WAN、SeerAnalyzer、License Server产品不涉及Webmin文件管理器模块权限提升漏洞。