

知 FW是否涉及Array Networks Array AG Series和xAG代码执行漏洞以及Array Networks ArrayOS AG安全漏洞

漏洞相关 王树岭 2023-11-30 发表

漏洞相关信息

漏洞编号: CVE-2023-28461、CVE-2023-41121

漏洞名称: Array Networks Array AG Series和xAG代码执行漏洞以及Array Networks ArrayOS AG安全漏洞

产品型号及版本: V7

漏洞描述

Array Networks ArrayOS AG是美国安瑞科技 (Array Networks) 公司的一个无论用户、设备或位置如何, 都可以实现安全远程访问的 SSL-VPN 产品。为任何用户、任何设备、任何地点提供对企业网络、企业应用程序和云服务的可扩展和可控的远程和移动访问。Array Networks Array AG Series 和 vxAG 9.4.0.481版本及之前版本允许远程代码执行。攻击者可以在没有身份验证的情况下使用HTTP标头中的 flags属性浏览SSL VPN网关上的文件系统。然后, 该产品可能会通过易受攻击的URL被利用。

Array Networks ArrayOS AG是美国安瑞科技 (Array Networks) 公司的一个无论用户、设备或位置如何, 都可以实现安全远程访问的 SSL-VPN 产品。为任何用户、任何设备、任何地点提供对企业网络、企业应用程序和云服务的可扩展和可控的远程和移动访问。Array Networks ArrayOS AG 9.4.0.499之前版本存在安全漏洞, 该漏洞源于允许攻击者通过异常的HTTP操作导致系统服务进程崩溃。

漏洞解决方案

不涉及