使用备用路径或通道进行身份验证绕过-CVE-2024-1709/CVE-2024-1708

漏洞相关 吴昊A 2024-02-28 发表

漏洞相关信息

漏洞编号： CVE-2024-1709/CVE-2024-1708
漏洞名称： 使用备用路径或通道进行身份验证绕过。
产品型号及版本： comware V7防火墙

漏洞描述

CVE-2024-1709: 使用备用路径或通道进行身份验证绕过。 漏洞成因： 在23.9.7及之前版本中， 未对路径“/SetupWizard.aspx”进行严格匹配。在C#的HttpRequest.Path中对于URL http://example.com/SetupWizard.aspx/abcd, 路径为/SetupWizard.aspx/abcd，从而命中“/SetupWizard.aspx”匹配， 导致身份验证绕过。 CVE-2024-1708: 路径穿越。 漏洞成因：在23.9.7及之前版本中，在解压应用扩展插件时为 对解压路径严格限制导致目录穿越。 根据已公开的PoC分析，远程代码执行利用过程如下： 1.使用合法用户登录或通过CVE-2024-1708绕过身份验证创建 用户。下图为通过CVE-2024-1709绕过身份验证添加用户。 2.通过添加扩展插件功能上传恶意扩展插件zip压缩包，其中 包含恶意ashx脚本代码。 3.访问/App_Extensions/下的恶意ashx脚本，实现远程命令执 行。 2. 影响版本 ConnectWise ScreenConnect <= 23.9.7 3. 缓解措施 1. 使用云服务用户， 无需任何操作， ConnectWise已将“screenconnect.com”云和“hostedrmm.com”中托管的ScreenConnect服务更新至23.9.8。 2.本地部署或自我托管的用户需将ScreenConnect更新至23.9.8版本

漏洞解决方案

comware V7安全产品不涉及