curl SOCKS5 堆溢出漏洞（CVE-2023-38545）通告

■ 通告编号	**NS-2023-0041**	■ 发布日期	**2023-10-11**
■ 漏洞危害	攻击者利用漏洞可实现任意代码执行		
■ **TAG**	curl、libcurl、CVE-2023-38545、CVE-2023-38546		

一. 漏洞概述

近日，绿盟科技监测到 curl 官方发布安全公告，修复了 SOCKS5 堆缓冲区溢出漏洞（CVE-2023-38545）和 cookie 注入漏洞（CVE-2023-38546）。漏洞细节已公开，请受影响用户尽快升级版本进行防护。

SOCKS5 堆缓冲区溢出漏洞（CVE-2023-38545）：

当要求 curl 将主机名传给 SOCKS5 代理进行地址解析时，若主机名超过 255 字节，curl 将会发生基于堆的缓冲区溢出。由于在缓慢的 SOCKS5 握手中，一个本地变量可能会产生错误值，导致 curl 不是复制已解析的地址，而是复制过长的主机名至目标缓冲区。此漏洞同时影响命令行工具 curl 和依赖库 libcurl。

cookie 注入漏洞（CVE-2023-38546）：

在特定条件下，攻击者可将 Cookie 插入到程序中。此漏洞是由于使用 curl_easy_duphandle 复制“easy handles”时，复制了 Cookie 使能状态，但未复制具体的 Cookies。这导致复制的句柄可能从后缀名为“none”的文件中加载 cookies。进而导致 Cookie 注入，因需满足多项条件，该漏洞风险较低，仅影响 libcurl。

cURL(客户端 URL)是一个开放源代码的命令行工具，用于在服务器之间传输数据，libcurl 是 curl 的一个流行和使用广泛的网络库，常用于编写网络应用程序和客户端，它提供了用于进行网络通信和数据传输的 API 和功能。

参考链接：

https://curl.se/docs/CVE-2023-38545.html

https://curl.se/docs/CVE-2023-38546.html

二. 影响范围

受影响版本

CVE-2023-38545

- 7.69.0 <= libcurl <= 8.3.0

CVE-2023-38546

- 7.9.1 <= libcurl <= 8.3.0

注：使用 libcurl 的操作系统和基于 cURL 和 libcurl 衍生的组件也受上述漏洞影响

不受影响版本

CVE-2023-38545/ CVE-2023-38546

- libcurl >= 8.4.0
- libcurl < 7.69.0

三. 漏洞防护

3.1 官方升级

目前官方已发布新版本修复上述漏洞，建议受影响用户及时更新升级进行防护：

https://curl.se/download.html

https://github.com/curl/curl/commit/fb4415d8aee6c1

3.2 临时缓解措施

1. 请勿设置 CURLPROXY_SOCKS5_HOSTNAME 启用代理；
2. 请勿将代理环境变量设置为 socks5h://

声明