

漏洞相关信息

漏洞编号: CVE-2021-35211

漏洞名称: 远程代码执行漏洞

产品型号及版本: SNA E1210、dc E3208、vdhcp E1104p01、license server E1151

漏洞描述



风险详情

基本情况描述

近日,美国网络安全厂商SolarWinds官方发布安全更新,修复了其FTP软件Serv-U的远程代码执行漏洞,漏洞编号为CVE-2021-35211。未授权的攻击者可利用该漏洞在目标服务器上执行任意代码。该漏洞仅影响启用了SSH协议的SolarWinds Serv-U Managed File Transfer及Serv-U Secure FTP, Serv-U环境中未启用SSH则不受此漏洞影响。请各单位组织排查,是否部署了受漏洞影响的SolarWinds产品,及时处置,做好安全加固工作。

漏洞影响范围: Serv-U <= 15.2.3 HF1

处置建议:

1.更新到安全版本

Serv-U 15.2.3 HF1 版本升级至 Serv-U 15.2.3 HF2;

Serv-U 15.2.3版本先升级至Serv-U 15.2.3 HF1,接着升级至Serv-U 15.2.3 HF2;

Serv-U 15.2.3 之前的所有Serv-U版本先升级至Serv-U 15.2.3,接着升级至Serv-U 15.2.3 HF1,然后再升级至 Serv-U 15.2.3 HF2。

2.缓解措施:

配置访问控制策略,避免受影响的Serv-U暴露在公网;在管理控制台中禁用SSH监听器。

SolarWinds官方公告链接: <https://www.solarwinds.com/trust-center/security-advisories/cve-2021-35211>

漏洞解决方案

不涉及

