

安全漏洞通告

SolarWinds 多个高危漏洞通告

360CERT

北京奇虎科技有限公司 | 2021-02-04

报告信息

报告名称	SolarWinds 多个高危漏洞通告		
报告类型	安全漏洞通告	报告编号	B6-2021-020401
报告版本	1	报告日期	2021-02-04
报告作者	360CERT	联系方式	cert@360.cn
提供方	北京奇虎科技有限公司		
接收方			

报告修订记录

报告版本	日期	修订	审核	描述
1	2021-02-04	360CERT	360CERT	撰写报告

目录

一、	漏洞档案	1
二、	漏洞简述	2
三、	漏洞评级	3
四、	漏洞详情	4
五、	相关空间测绘数据	5
六、	影响版本	6
七、	安全建议	7
(一)	通用修补方案	7
(二)	临时修补方案	7
八、	产品侧解决方案	8
(一)	360 城市级网络安全监测服务	8
九、	参考链接	9
附录 A	报告风险等级说明	10
附录 B	影响面说明	12
附录 C	360 内部评分体系	13

一、漏洞档案



漏洞类型	安全配置错误漏洞
CVE 编号	CVE-2021-25276 等
相关厂商	Solarwinds
相关组件	暂无
威胁等级	高危
影响面	一般
360CERT 评分	8.5
修复方案	通用修补方案/临时修补方案
漏洞发布时间	2021-02-04
报告生成时间	2021-02-04

二、漏洞简述

2021年02月04日，360CERT监测发现 Trustwave 发布了 SolarWinds 安全漏洞 的风险通告，漏洞等级：高危，漏洞评分：8.5。

SolarWinds 修复了 Orion 平台以及 ServU-FTP 中的三处漏洞，分别造成远程代码执行、数据库失陷及数据泄漏、本地磁盘文件读写影响。

对此，360CERT 建议广大用户及时将 SolarWinds 升级到最新版本。与此同时，请做好资产自查以及预防工作，以免遭受黑客攻击。

三、漏洞评级

经过安全技术人员的分析，最终对该漏洞的评定结果如下

评定方式	等级
威胁等级	高危
影响面	一般
360CERT 评分	8.5

四、漏洞详情

CVE-2021-25275: 代码执行漏洞

SolarWinds Orion 平台开放的 1801 端口是 MSSQL 消息队列允许未授权访问，攻击者发送恶意请求至该消息队列，触发反序列化造成远程代码执行。

CVE-2021-25276: 信息泄漏漏洞

SolarWinds 中存在一处访问控制漏洞，攻击者可以直接访问并控制后端数据库 SOLARWINDS_ORION 。攻击者可以查询该数据库中的一切数据造成信息泄漏。

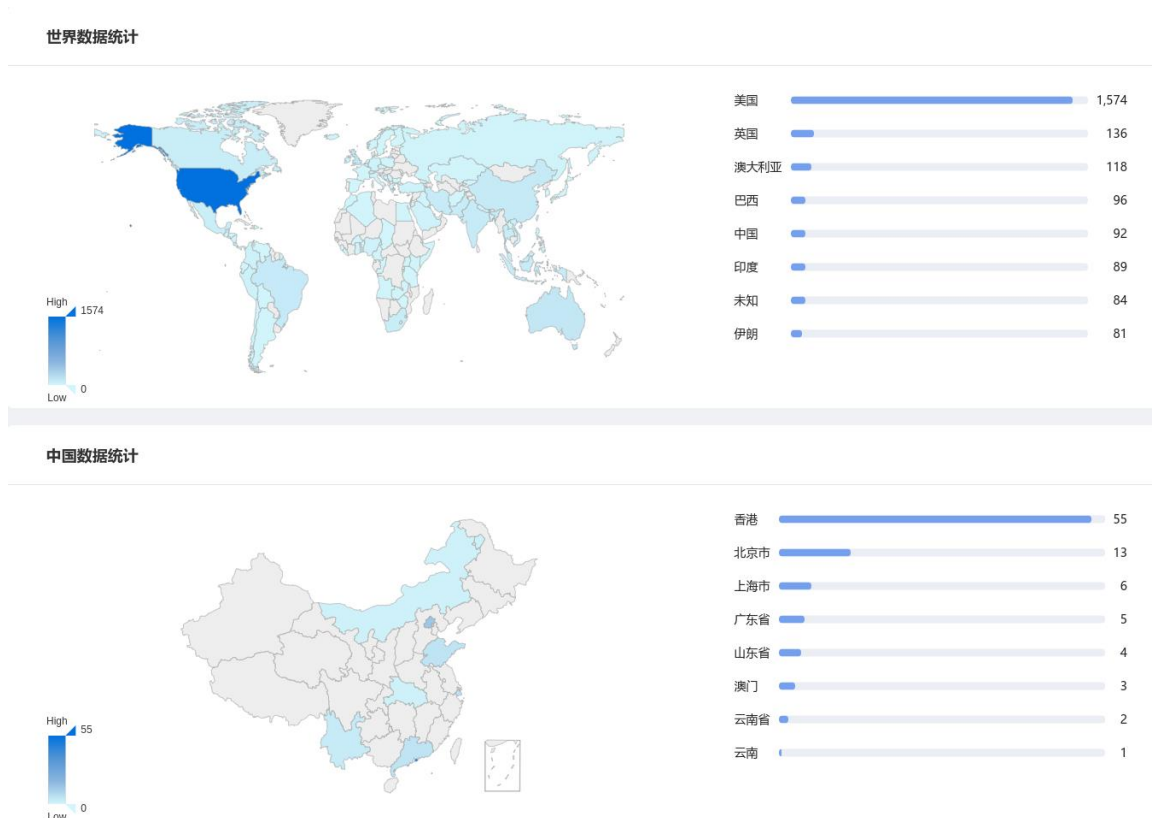
CVE-2021-25276: 安全配置错误漏洞

SolarWinds 的 Serv-FTP 组件配置不当，任何通过身份验证的用户将获得该系统所在计算机 C 盘（系统目录）的完全控制权限，可以任意上传下载文件。

五、 相关空间测绘数据

360 安全大脑-Quake 网络空间测绘系统通过对全网资产测绘，发现

SolarWinds Orion 具体分布如下图所示。



六、影响版本

产品名称	影响版本
serv_u_ftp	<15.2.2 Hotfix 1
orion	<2020.2.4

360CERT

七、安全建议

(一) 通用修补方案

升级 SolarWinds 组件至以下版本

- SolarWinds Orion2020.2.4
- SolarWinds Serv-FTP 15.2.2 Hotfix 1

(二) 临时修补方案

1. 关闭 TCP 1801 端口
2. 关闭 FTP 端口（默认情况下为 21/22）

八、产品侧解决方案

(一) 360 城市级网络安全监测服务

360CERT 的安全分析人员利用 360 安全大脑的 QUAKE 资产测绘平台

(quake.360.cn)，通过资产测绘技术的方式，对该漏洞进行监测。可联系相关产品区域负责人或(quake#360.cn)获取对应产品。



九、 参考链接

1. SolarWinds patches three newly discovered software vulnerabilities

<https://www.zdnet.com/article/solarwinds-patches-three-newly-discovered-software-vulnerabilities/>

2. Full System Control with New SolarWinds Orion-based and Serv-U FTP Vulnerabilities

<https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/full-system-control-with-new-solarwinds-orion-based-and-serv-u-ftp-vulnerabilities/>

附录 A 报告风险等级说明

360CERT 评分是依托 CVSS3.1 的评价体系，由 360CERT 进行分数评定的危害评分

严重	
评定标准	1. $9.0 \leq 360\text{CERT 评分} \leq 10$ 2. Top20 组件 3. PoC/Exp 公开可直接利用 4. 获得系统权限 5. 蠕虫性攻击
危害结果	1. 任意攻击者可直接发起攻击 2. 直接获得服务器控制权限 3. 直接影响业务服务运行 4. 核心敏感数据泄漏 5. 下载任意文件 6. 易造成资金风险
修复建议	建议在 3 个工作日内对涉及的产品/组件进行修复操作

高危	
评定标准	1. $7.0 \leq 360\text{CERT 评分} < 9$ 2. 通用组件 3. PoC 公开 4. 获得服务/数据库权限
危害结果	1. 系统/服务/资源垂直越权 2. 获得数据库权限 3. 可造成资金风险
修复建议	建议在 7 个工作日内对涉及的产品/组件进行修复操作

中危	
评定标准	<ol style="list-style-type: none"> 1. $4.0 \leq 360\text{CERT 评分} < 7$ 2. 需要额外的操作步骤方可实现攻击 3. 对服务的运行产生影响但不影响功能 <ol style="list-style-type: none"> a) 占用存储空间 b) 降低执行效率 4. 获得平台用户级权限
危害结果	<ol style="list-style-type: none"> 1. 需要额外的操作步骤实现危害行为 2. 获得平台平行越权 3. 任意文件上传 4. 难造成资金风险
修复建议	建议在 12 个工作日内对涉及的产品/组件进行修复操作

低危	
评定标准	<ol style="list-style-type: none"> 1. $0 \leq 360\text{CERT 评分} < 4$ 2. 不对服务的运行产生影响
危害结果	暂无
修复建议	建议在 20 个工作日内对涉及的产品/组件进行修复操作

附录 B 影响面说明

影响面说明	
广泛	影响主体数 > 10w 底层依赖库
一般	5w < 影响主体数 < 10w 开源库
局限	影响主体数 < 5w 特制版本的

附录 C 360 内部评分体系

360 内部评分体系是 360CERT 安全研究人员经过一系列的数据分析和调查研究，并结合多年的漏洞研究经验最终得出的一套针对漏洞和安全事件的科学评分标准。此套评分体系能够用来评测漏洞和安全事件的严重程度，并帮助确定所需反应的紧急度和重要度。经验证，此评分体系适用于市面上几乎所有的漏洞和安全事件。

360 内部评分体系建立在“CVSS 漏洞评分体系”的基础上，其最终分数是取决于多个指标的公式，最终计算得出的近似的漏洞利用容易程度和漏洞利用的影响。分数范围是 0 到 10，其中最严重的是 10。该分数能较直观地反映漏洞的威胁等级，具体对应规则如下：

分数	威胁等级
9.0 - 10.0	严重
7.0 - 8.9	高危
4.0 - 6.9	中危
0 - 3.9	低危