漏洞事件通告

SolarWinds 供应链攻击通告

360CERT
北京奇虎科技有限公司 | 2020-12-14

报告信息

报告名称	SolarWinds 供应链攻击通告		
报告类型	漏洞事件通告	**报告编号**	B6-2020-121403
报告版本	1	**报告日期**	2020-12-14
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	2020-12-14	360CERT	360CERT	撰写报告

目录

一、 事件档案 1
二、 事件简述 2
三、 事件评级 3
四、 事件详情 4
五、 安全建议 6
(一) 通用修补方案 6
(二) 临时修补方案 6
六、 产品侧解决方案 7
七、 参考链接 8
附录 A 报告风险等级说明 9
附录 B 影响面说明 11
附录 C 360 内部评分体系 12

一、 事件档案

漏洞类型	无类型
CVE 编号	无
相关厂商	SolarWinds
相关组件	SolarWinds
威胁等级	严重
影响面	广泛
360CERT 评分	10
修复方案	通用修补方案/临时修补方案
事件发布时间	2020-12-13
报告生成时间	2020-12-14

二、事件简述

2020 年 12 月 14 日，360CERT 监测发现 FireEye 发布了 SolarWinds 供应链攻击通告 的分析报告，事件等级：严重，事件评分：10。

SolarWInds 的产品中存在长达 1 年的供应链攻击，其产品中被植入多个后门。

后门程序于 2020 年 3 月已经被 SolarWInds 官方应用程序引入，使用 SolarWinds 的用户需要立即安装更新修复

对此，360CERT 建议广大用户好资产自查以及预防工作，以免遭受黑客攻击。

三、 事件评级

经过安全技术人员的分析，最终对该事件的评定结果如下

评定方式	等级
威胁等级	严重
影响面	广泛
360CERT 评分	10

四、 事件详情

SolarWinds Inc.是一家美国公司，为企业提软件以帮助管理其网络，系统和信息技术基础架构。根据其官网简介，SolarWinds 的客户包括了"财富美国 500 强"（Fortune 500）企业、美国所有前十大电信业者、美军所有五大部队、美国国务院、国家安全局，以及美国总统办公室等。

根据 SolarWinds 官方发布安全公告，SolarWinds Orion 平台软件在 2020 年 3 月至 6 月之间发布的 2019.4 - 2020.2.1 版本都受到了供应链攻击的影响，这些版本的安装包内存在恶意的后门应用程序。

这些安装程序通过 SolarWinds 的数字证书绕过了检查。安装更新后会释放一个 SolarWinds.Orion.Core.BusinessLayer.dll 文件，该文件被 Orion 平台通过 SolarWinds.BusinessLayerHostx[64].exe 当作额外的插件进行加载。

该后门在经过长达两个星期的休眠期后，会根据 C2 返回的指令进行活动。（包括传输文件，执行文件，对系统进行配置文件，重新引导计算机以及禁用系统服务）

同时该恶意程序的所有网络通信都会伪装成 Orion Improvement Program（OIP）协议的网络流量，并将通信返回结果存储在合法的插件配置文件中，从而使其能够无缝的与 SolarWinds 自身活动融合。进而达到隐蔽的目的。

相关文件:

- CORE-2019.4.5220.20574-SolarWinds-Core-v2019.4.5220-Hotfix5.msp（02af7cec58b9a5da1c542b5a32151ba1）

SolarWinds 升级程序中也包含了该后门应用程序，系统管理员若在 2020 年 3 月-6 月期间安装过更新，受到该次攻击影响。

五、 安全建议

(一) 通用修补方案

升级到 2020.2.1 HF 1

并于 2020 年 12 月 15 日升级到 2020.2.1 HF2

SolarWinds 为商业软件请联系 swisupport#solarwinds.com 获取支持

(二) 临时修补方案

目前 360 安全大脑、360 情报云等 360 政企全线安全产品可以检测和防御 SolarWinds 软件供应链攻击。

360 安全大脑已提供 SolarWinds 供应链后门专杀工具，请联系 ata@360.cn 获取。

六、 产品侧解决方案

(一) 360 安全大脑

目前 360 安全大脑、360 情报云等 360 政企全线安全产品可以检测和防御 SolarWinds 软件供应链攻击。

360 安全大脑已提供 SolarWinds 供应链后门专杀工具 ， 请联系 ata#360.cn 获取。

七、 参考链接

1. SolarWinds 供应链攻击报告

   https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html

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 ≤ 360CERT 评分 ≤ 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 ≤ 360CERT 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	1. 4.0 ≤ 360CERT 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 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	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	1. 0 ≤ 360CERT 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