安全事件周报

安全事件周报 (12.28-01.03)

360CERT

360CERT
北京奇虎科技有限公司 | 2021-01-04

报告信息

报告名称	安全事件周报（12.28-01.03）		
报告类型	安全事件周报	报告编号	B6-2021-010401
报告版本	1.0	报告日期	2021-01-04
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
1.0	2021-01-04	360CERT	360CERT	撰写报告

360CERT

目录

360CERT

一、 事件概览

本周收录安全事件 26 项

话题集中在`网络攻击`、`数据泄露`方面，涉及的组织有：`SolarWinds`、`Chrome`、`GitHub`、`日本川崎重工`等。数据窃取贩卖频发，数据防护不可忽视。

对此，360CERT 建议：

1. 使用 360 安全卫士进行病毒检测、
2. 使用 360 安全分析响应平台进行威胁流量检测，
3. 使用 360 城市级网络安全监测服务 QUAKE 进行资产测绘，
4. 做好资产自查以及预防工作，以免遭受黑客攻击。

二、 事件档案

恶意程序	**等级**
基于 GitHub 的恶意软件从 Imgur pic 下载恶意脚本	★★★★
Nefilim 勒索软件运营商泄露从 Whirlpool 窃取的数据	★★★★
新的基于 AutoHotkey 的恶意软件针对美国、加拿大银行	★★★★
Wasabi 云存储服务因托管恶意软件而被下线	★★★
新的蠕虫病毒把 Windows、Linux 服务器变成了 Monero 矿工	★★★
数据安全	**等级**
电子商务应用程序 21 Buttons 公开数百万用户的数据	★★★★★
日本川崎重工披露可能造成数据泄露的安全漏洞	★★★★
慈善机构 Get Schooled 遭受数据泄露	★★★★
数据代理公司出售 26 家公司的用户记录	★★★
T-Mobile 数据泄露暴露电话号码、通话记录	★★
网络攻击	**等级**
越南成为供应链攻击的目标	★★★★★
SolarWinds 黑客访问了微软的源代码	★★★★★
在`Shopify`、`BigCommerce`等商店发现跨平台的信用卡窃取器	★★★★
黑客加强了 COVID-19 知识产权盗窃攻击力度	★★★★
SolarWinds 黑客的目标是访问受害者的云资产	★★★★
FBI：攻击者劫持智能设备	★★★★
Voyager 加密货币交易平台因网络攻击而暂停交易	★★★★
芬兰称黑客访问了国会议员的电子邮件帐户	★★★
Ticketmaster 因侵入竞争对手的系统而被罚款 1000 万美元	★★★
金融服务业每天遭受数千万次攻击	★★★

360CERT

其他事件	等级
超一百万个 Zyxel 防火墙、VPN 网关中存在后门帐户	★★★★★
英国警方在网络打击行动中逮捕了 21 名 WeLeakInfo 用户	★★★★
CISA 发布工具，用以检测 Azure/Microsoft 365 环境中的恶意活动	★★★
Google Docs 的漏洞允许黑客访问私人文档	★★★
CISA 发布有关 SolarWinds 补丁的新指南	★★★
Chrome 修复了 Windows10 上的防病毒"文件锁定"错误	★★

360CERT

三、 事件详情

(一) 恶意程序

基于 GitHub 的恶意软件从 Imgur pic 下载恶意脚本

日期: 2020-12-28

等级: 高

来源: Ax Sharma

标签: ['PowerShell', 'GitHub', 'Macros', 'Cobalt Strike', 'Imgur pic', 'MuddyWater']

一个新的恶意软件使用带有宏的 Word 文件从 GitHub 下载 PowerShell 脚本。
此 PowerShell 脚本进一步从图像托管服务 Imgur 下载合法的图像文件，以在 Windows 系统上执行 Cobalt Strike 脚本。
研究人员根据已知的信息，将该恶意软件与`MuddyWater`（又名`SeedWorm`）相关联，后者是政府支持的高级持续威胁（`APT`）小组。

详情

GitHub-based malware calculates Cobalt Strike payload from Imgur pic
https://www.bleepingcomputer.com/news/security/github-based-malware-calculates-cobalt-strike-payload-from-imgur-pic/

Nefilim 勒索软件运营商泄露从 Whirlpool 窃取的数据

日期: 2020-12-28

等级: 高

来源: Pierluigi Paganini

标签: ['American', 'Nefilim', 'Whirlpool', 'Ransomware']

美国跨国家电生产商和批发商`Whirlpool`遭受了勒索软件攻击，`Nefilim`勒索软件运营商声称从公司那里窃取了数据，并威胁说如果公司不支付赎金，便会泄漏所有的数据。
与`Whirlpool`高管的谈判失败后，`Nefilim`泄漏了数据，第一批数据包括员工福利、住宿要求、医疗信息要求和其他信息相关的文件。
该公司在全球 59 个制造和技术研究中心拥有 77,000 多名员工。

详情

Nefilim ransomware operators leak data stolen from Whirlpool
https://securityaffairs.co/wordpress/112722/cyber-crime/whirlpool-nefilim-ransomware.html

新的基于 AutoHotkey 的恶意软件针对美国、加拿大银行

日期: 2020-12-30

等级: 高

来源: Akshaya Asokan

标签: ['AutoHotkey', 'Credentials', 'Browser']

研究人员发现了一种新的 infostealer 恶意软件，它是用自动热键编程语言编写的，能够从不同的 web 浏览器中窃取银行凭证。这项攻击活动在美国和加拿大各地都很活跃，目标客户包括 Scotia Bank、PayPal、加拿大皇家银行、Capital One 和汇丰银行等。

详情

New AutoHotkey-Based Malware Targets US, Canadian Banks

https://www.databreachtoday.com/new-autohotkey-based-malware-targets-us-canadian-banks-a-15680

Wasabi 云存储服务因托管恶意软件而被下线

日期: 2020-12-29

等级: 中

来源: Lawrence Abrams

标签: ['Wasabi', 'Cloud storage', 'Amazon S3', 'Malware']

云存储提供商`Wasabi`遭遇了一次服务中断，原因是用于存储端点的域托管了恶意软件。Wasabi 是一家云存储提供商，提供便宜的服务，不收取出口或 API 费用，并保证数据持久性。
2020 年 12 月 28 日，Wasabi 用户突然发现他们不能再访问托管在 wasabisys.com 域名上的数据。
Wasabi 称目前正在调查。

详情

Wasabi cloud storage service knocked offline for hosting malware

https://www.bleepingcomputer.com/news/security/wasabi-cloud-storage-service-knocked-offline-for-hosting-malware/

新的蠕虫病毒把 Windows、Linux 服务器变成了 Monero 矿工

日期: 2020-12-30

等级: 中

来源: Sergiu Gatlan

标签: ['Windows', 'Linux', 'Golang', 'ELF Malware', 'Brute Force']

自 2020 年 12 月初以来，一种新发现并自我传播的基于 Golang 的恶意软件一直积极地在 Windows 和 Linux 服务器上下放 XMRig 加密货币矿工。这种多平台恶意软件通过对面向公众的服务（即 MySQL，Tomcat，Jenkins 和 WebLogic）进行暴力破解，将其传播到其他系统。

详情

New worm turns Windows, Linux servers into Monero miners

https://www.bleepingcomputer.com/news/security/new-worm-turns-windows-linux-servers-into-monero-miners/

相关安全建议

1. 在网络边界部署安全设备，如防火墙、IDS、邮件网关等
2. 减少外网资源和不相关的业务，降低被攻击的风险
3. 各主机安装 EDR 产品，及时检测威胁
4. 及时对系统及各个服务组件进行版本升级和补丁更新
5. 包括浏览器、邮件客户端、vpn、远程桌面等在内的个人应用程序，应及时更新到最新版本
6. 勒索中招后，应及时断网，并第一时间联系安全部门或公司进行应急处理

(二) 数据安全

电子商务应用程序 21 Buttons 公开数百万用户的数据

日期: 2020-12-28

等级: 高

来源: Pierluigi Paganini

标签: ['21 Buttons', 'Europe', 'AWS bucket', 'vpnMentor', 'E-commerce']

网络安全公司`vpnMentor`的研究人员发现，电子商务应用程序`21 Buttons`正在公开用户的私人数据。
`21 Buttons`允许用户共享其所穿衣服的照片以及指向所穿品牌的链接，然后其关注者可以使用该应用直接从相关品牌购买自己喜欢的衣服。
2020 年 11 月 2 日，`vpnMentor`专家发现`21 Buttons`应用程序使用了配置错误的`AWS`存储库，该存储库包含超过 5000 万个文件，包括许多敏感信息，如全名、地址、财务信息、照片和视频等。

详情

E-commerce app 21 Buttons exposes millions of users' data
https://securityaffairs.co/wordpress/112701/data-breach/button-21-data-leak.html

日本川崎重工披露可能造成数据泄露的安全漏洞

日期: 2020-12-29

等级: 高

来源: Sergiu Gatlan

标签: ['Japan', 'Kawasaki Heavy Industries', 'Japanese', 'Data Leak', 'Unauthorized', 'Security Breach']

日本川崎重工（Kawasaki Heavy Industries）披露了一项安全漏洞，利用该漏洞，攻击者可能在未授权的情况下从多个海外办事处访问日本公司的服务器。
川崎重工是一家日本跨国公司，拥有 35,000 多名员工，活跃于重型设备，机车车辆，汽车，航空航天和国防工业。
川崎重工在 2020 年 12 月 28 日发表的一份声明中说，经过彻底的调查，该公司发现海外办事处的某些信息可能已经泄露给外部各方。

详情

Kawasaki discloses security breach, potential data leak

https://www.bleepingcomputer.com/news/security/kawasaki-discloses-security-breach-potential-data-leak/

慈善机构 Get Schooled 遭受数据泄露

日期: 2020-12-31

等级: 高

来源: Derek B. Johnson

标签: ['AWS', 'TurgenSec', 'Get Schooled', 'AWS bucket']

纽约一家慈善机构 Get Schooled 遭受了数据泄露，导致与数十万名学生相关的记录留在了一个不安全的 AWS bucket 中，该 bucket 是开放的，可以从互联网访问。这些公开的数据包括与该非营利组织有关的学生的详细信息，包括姓名、电子邮件、年龄、性别、高中或大学以及毕业数据、实际地址和电话号码。

详情

Non-profit founded by Gates Foundation suffers massive exposure of student records

https://www.scmagazine.com/home/security-news/student-college-non-profit-founded-by-gates-foundation-suffers-student-records-breach/

数据代理公司出售 26 家公司的用户记录

日期: 2020-12-31

等级: 中

来源: Lawrence Abrams

标签: ['Data breach broker']

一家数据代理公司开始在黑客论坛上出售 26 家公司总计 36.88 万条被盗用户记录。当攻击者和黑客组织破坏一家公司并窃取其用户数据库时，他们通常会与数据代理公司合作，后者为他们推销数据。经纪人随后会在黑客论坛和黑暗网络市场上发布帖子，推销被盗数据。

详情

Data breach broker selling user records stolen from 26 companies

https://www.bleepingcomputer.com/news/security/data-breach-broker-selling-user-records-stolen-from-26-companies/

T-Mobile 数据泄露暴露电话号码、通话记录

日期: 2020-12-30

等级: 中

来源: Lawrence Abrams

标签: ['CPNI', 'T-Mobile']

据 T-Mobile 称，其安全团队最近发现了对其系统的恶意攻击。在网络安全公司进行调查后发现，攻击者获得了由客户生成的电信信息，即 CPNI。这次泄露的信息包括电话号码、通话记录和账户上的线路数。“访问了联邦通信委员会（FCC）规定的客户专有网络信息（CPNI）。T-Mobile 在一份数据泄露通知中表示：“访问的 CPNI 可能包括电话号码、您

账户上订阅的线路数，在某些情况下，还包括作为您无线服务正常运行的一部分而收集的与通话相关的信息。”。

详情

T-Mobile data breach exposed phone numbers, call records

https://www.bleepingcomputer.com/news/security/t-mobile-data-breach-exposed-phone-numbers-call-records/

相关安全建议

1. 及时备份数据并确保数据安全
2. 及时检查并删除外泄敏感数据
3. 合理设置服务器端各种文件的访问权限
4. 条件允许的情况下，设置主机访问白名单

(三) 网络攻击

越南成为供应链攻击的目标

日期: 2020-12-28

等级: 高

来源: Catalin Cimpanu

标签: ['Vietnamese', 'the Vietnam Government Certification Authority', 'Supply Chain Attack', 'ESET', 'Certificate']

一群黑客通过在政府软件工具包中插入恶意软件，对越南的私营公司和政府机构实施了一次巧妙的供应链攻击。
该攻击是由安全公司 ESET 发现的，并在名为`Operation SignSight`的报告中进行了详细描述。攻击的对象是越南政府证书颁发机构（`VGCA`），该政府组织颁发可以用于电子签名正式文件的数字证书。
但是 ESET 表示，2020 年某个时候，黑客入侵了该机构位的的网站`ca.gov.vn`，并将恶意软件插入了两个`VGCA`客户端应用程序中，这些应用程序可供在该网站上下载。
ESET 表示，在 2020 年 7 月 23 日至 8 月 5 日期间，这两个文件包含了一个名为`PhantomNet`的后门木马。

详情

Vietnam targeted in complex supply chain attack

https://www.zdnet.com/article/vietnam-targeted-in-complex-supply-chain-attack/

SolarWinds 黑客访问了微软的源代码

日期: 2020-12-31

等级: 高

来源: Catalin Cimpanu

标签: ['SolarWinds', 'Microsoft', 'Source Code']

SolarWinds 供应链攻击背后的黑客成功访问了对微软内部网络，并获得了少量内部账户的访问权限，这些账户使他们可以访问微软源代码库。微软表示，黑客并没有对他们访问的存储库进行任何更改，因为被泄露的账户只有查看代码的权限，而没有修改代码的权限。微软强调，尽管黑客查看了一些源代码，但攻击者并没有将攻击升级到生产系统、客户数据或使用微软产品攻击微软客户。

详情

SolarWinds hackers accessed Microsoft source code

https://www.zdnet.com/article/solarwinds-hackers-accessed-microsoft-source-code/

在`Shopify`、`BigCommerce`等商店发现跨平台的信用卡窃取器

日期: 2020-12-28

等级: 高

来源: Sergiu Gatlan

标签: ['Shopify', 'MageCart', 'E-Commerce Platform', 'Skimmer', 'Payment Card']

最近发现的跨平台信用卡窃取器可以在`Shopify`，`BigCommerce`，`Zencart`和`Woocommerce`的商店中收集付款信息。
这种恶意软件通常是针对单一类型的电子商务平台设计的，但这种新型的网络恶意软件可以通过注入恶意的结账页面，接管多个商店的结账过程。
该窃取器通过在客户登陆真实的结帐页面之前显示一个伪造的付款页面，并使用键盘记录器拦截付款和个人信息来做到这一点。

详情

Multi-platform card skimmer found on Shopify, BigCommerce stores

https://www.bleepingcomputer.com/news/security/multi-platform-card-skimmer-found-on-shopify-bigcommerce-stores/

黑客加强了 COVID-19 知识产权盗窃攻击力度

日期: 2020-12-28

等级: 高

来源: Tara Seals

标签: ['IP', 'Pfizer', 'Moderna', 'COVID-19', 'Zebrocy', 'Vaccine Supply Chain']

随着对`COVID-19`疫苗的研究发展，`Pfizer`公司，`Moderna`公司和其他生物技术公司开始大量生产疫苗，攻击者现在将医疗保健空间视为一个丰富的知识产权（IP）库。
网络攻击最近集中在`COVID-19`疫苗供应链上，黑客继续使用`Zebrocy`恶意软件进行与疫苗相关的网络攻击。2020 年 12 月，攻击者获取了辉瑞和生物技术公司提交给欧盟监管机构的疫苗文件。

详情

Hackers Amp Up COVID-19 IP Theft Attacks

https://threatpost.com/hackers-amp-up-covid-19-ip-theft-attacks/162634/

SolarWinds 黑客的目标是访问受害者的云资产

日期: 2020-12-29

等级: 高

来源: Pierluigi Paganini

标签: ['Microsoft', 'SolarWinds', 'Solorigate', 'Cloud', 'Backdoor', 'SAML', 'Supply Chain Attack']

`Microsoft 365 Defender`团队透露，`SolarWinds`供应链攻击的目标是受害者的云资产，一旦 `Sunburst/Solorigate` 后门感染了受害者的网络，攻击者便将其转移到受害者的云基础架构。
一旦部署了后门，攻击者就可以使用它来窃取凭据，提升特权并在目标网络内进行横向移动，从而获得创建有效`SAML`令牌的能力。
接着，攻击者就可以利用`SAML`令牌来访问云资源并泄露电子邮件和敏感数据。

详情

SolarWinds hackers aimed at access to victims' cloud assets
https://securityaffairs.co/wordpress/112773/hacking/solarwinds-solorigate-attack-chain.html

FBI：攻击者劫持智能设备

日期: 2020-12-29

等级: 高

来源: Catalin Cimpanu

标签: ['FBI', 'Smart Devices', 'Hijacking', 'Leaked']

美国联邦调查局(FBI)表示，攻击者劫持了安全保障薄弱的智能设备，包括具有视频和音频功能的家庭监控设备。
攻击者正在接管一些设备，这些设备的所有者在这些设备上创建了帐户，但重复使用了以前在其他公司的数据泄露出来的凭据。

详情

FBI: Pranksters are hijacking smart devices to live-stream swatting incidents

https://www.zdnet.com/article/fbi-pranksters-are-hijacking-smart-devices-to-live-stream-swatting-incidents/

Voyager 加密货币交易平台因网络攻击而暂停交易

日期: 2020-12-29

等级: 高

来源: Lawrence Abrams

标签: ['Voyager', 'Cryptocurrency Broker', 'DNS', 'Cyberattack']

Voyager 加密货币交易平台于 12 月 28 日暂停了交易，因为其 DNS 配置遭到了网络攻击。
Voyager Digital LLC 是一家加密货币交易平台，允许投资者使用 Voyager 移动应用程序交易资产。Voyager 2020 年增长迅速，在 12 个月内增长了 40 倍，管理的资产为 2 亿美元。

详情

Voyager cryptocurrency broker halted trading due to cyberattack

https://www.bleepingcomputer.com/news/security/voyager-cryptocurrency-broker-halted-trading-due-to-cyberattack/

芬兰称黑客访问了国会议员的电子邮件帐户

日期: 2020-12-28

等级: 中

来源: Catalin Cimpanu

标签: ['Parliament', 'IT System', 'APT28', 'Finland', 'MPs', 'Emails Accounts']

芬兰议会 2020 年 12 月 28 日表示，黑客入侵了其内部 IT 系统，并访问了一些国会议员的电子邮件帐户。
政府官员说，袭击发生在 2020 年秋天，是 12 月由议会 IT 人员发现的。 芬兰中央刑事警察（KRP）目前正在调查此事。
`KRP`专员`Tero Muurman`在一份正式声明中说，这次袭击并未对议会内部的`IT`系统造成任何损害。

详情

Finland says hackers accessed MPs' emails accounts

https://www.zdnet.com/article/finland-says-hackers-accessed-mps-emails-accounts/

Ticketmaster 因侵入竞争对手的系统而被罚款 1000 万美元

日期: 2020-12-31

等级: 中

来源: Sergiu Gatlan

标签: ['Ticketmaster', 'Live Nation', 'CrowdSurge']

Ticketmaster 是 Live Nation 的子公司，也是一家领先的票务分销和销售公司，因使用其一名前雇员的证件非法访问竞争对手 CrowdSurge 的系统而被罚款 1000 万美元。该员工在加入 Live Nation 后，为 TicketMaster 高管使用的票务网页草稿共享了私有的 CrowdSurge URL。

详情

Ticketmaster fined $10 million for breaking into rival's systems

https://www.bleepingcomputer.com/news/security/ticketmaster-fined-10-million-for-breaking-into-rival-s-systems/

金融服务业每天遭受数千万次攻击

日期: 2020-12-31

等级: 中

来源: Steve Zurier

标签: ['Akamai', 'Financial', 'CyberAttack']

在更新的互联网现状报告中显示，在过去一年中，金融服务行业每天遭受数百万或数千万次攻击。仅在 2020 年 9 月，就追踪到 3300 万起针对金融服务行业的 web 应用程序攻击。报告发现，攻击者主要使用常见的攻击路径，如 SQL 注入、本地文件包含和跨站点脚本。

详情

Financial services industry hit with tens of millions of attacks per day

https://www.scmagazine.com/home/security-news/financial-services-industry-hit-with-tens-of-millions-of-attacks-per-day/

相关安全建议

1. 做好资产收集整理工作，关闭不必要且有风险的外网端口和服务，及时发现外网问题
2. 积极开展外网渗透测试工作，提前发现系统问题
3. 及时对系统及各个服务组件进行版本升级和补丁更新
4. 包括浏览器、邮件客户端、vpn、远程桌面等在内的个人应用程序，应及时更新到最新版本
5. 软硬件提供商要提升自我防护能力，保障供应链的安全

(四) 其他事件

超一百万个 Zyxel 防火墙、VPN 网关中存在后门帐户

日期: 2021-01-02

等级: 高

来源: Catalin Cimpanu

标签: ['Zyxel', 'VPN', 'Firewall']

超过一百万个 Zyxel 防火墙、VPN 网关和访问点控制器包含一个硬编码的管理级后门帐户，该帐户可以通过 SSH 接口或 web 管理面板授予攻击者对设备的根访问权限。
受影响的型号包括 Zyxel 的许多顶级产品，包括：
- 高级威胁防护（ATP）系列-主要用作防火墙
- 统一安全网关（USG）系列-用作混合防火墙和 VPN 网关
- USG FLEX 系列-用作混合防火墙和 VPN 网关
- VPN 系列-用作 VPN 网关
- NXC 系列-用作 WLAN 接入点控制器

详情

Backdoor account discovered in more than 100,000 Zyxel firewalls, VPN gateways

https://www.zdnet.com/article/backdoor-account-discovered-in-more-than-100000-zyxel-firewalls-vpn-gateways/

英国警方在网络打击行动中逮捕了 21 名 WeLeakInfo 用户

日期: 2020-12-28

等级: 高

来源: Prajeet Nair

标签: ['U.K.', 'Britain', 'WeLeakInfo', 'Cyber Crackdown']

英国国家犯罪局（National Crime Agency）称，英国警方已经逮捕了 21 人，他们是现已倒闭的`WeLeakInfo`网站的客户，该网站为网络罪犯提供了超过 120 亿份的个人记录，这些数据是从 1 万个数据库中违规获取的。
在运营期间，`WeLeakInfo`向犯罪分子出售帐户的名称，电子邮件地址，用户名，电话号码和密码等，这些犯罪分子每天将以低至 2 美元的价格购买订阅，以访问数据。

详情

UK Police Arrest 21 WeLeakInfo Users In Cyber Crackdown

https://www.databreachtoday.com/uk-police-arrest-21-weleakinfo-users-in-cyber-crackdown-a-15666

CISA 发布工具，用以检测 Azure/Microsoft 365 环境中的恶意活动

日期: 2020-12-28

等级: 中

来源: Sergiu Gatlan

标签: ['CISA', 'PowerShell-based', 'Azure', 'Microsoft 365', 'Tool']

网络安全和基础结构安全局（CISA）发布了基于`PowerShell`的工具，该工具可帮助检测`Azure/Microsoft 365` 环境中可能受到威胁的应用程序和帐户。
在此之前，`Microsoft` 披露了攻击者如何利用窃取的凭据和访问令牌来登陆`Azure`客户。该工具旨在供事件应急响应人员使用，仅检测基于身份验证攻击的活动。

详情

CISA releases Azure, Microsoft 365 malicious activity detection tool

https://www.bleepingcomputer.com/news/security/cisa-releases-azure-microsoft-365-malicious-activity-detection-tool/

Google Docs 的漏洞允许黑客访问私人文档

日期: 2020-12-29

等级: 中

来源: The Hacker News

标签: ['Google Docs', 'Vulnerability', 'Screenshots', 'Private Documents', 'Cloud', 'Iframe']

谷歌修复了其服务集成的反馈工具中的一个漏洞，攻击者可以利用该漏洞将该反馈工具嵌入到恶意网站中，从而窃取`Google Docs`文档的截图。
该漏洞于 7 月 9 日被安全研究员`Sreeram KL`发现，他因此获得了 Google 漏洞奖励计划的 3133.70 美元。

详情

A Google Docs Bug Could Have Allowed Hackers See Your Private Documents

https://thehackernews.com/2020/12/a-google-docs-bug-could-have-allowed.html

CISA 发布有关 SolarWinds 补丁的新指南

日期: 2020-12-31

等级: 中

来源: Akshaya Asokan

标签: ['SolarWinds', 'CISA']

CISA 要求各大机构在 12 月 31 日前更新到最新版本网络安全和基础设施安全局发布紧急指令，要求所有仍在运行易受攻击的 SolarWinds Orion 软件的联邦组织立即更新至最新版本。CISA 称：“国家安全局已经检查了这个版本，并验证了它消除了先前发现的恶意代码，”

详情

CISA Releases New Guidance on SolarWinds Patch

https://www.databreachtoday.com/cisa-releases-new-guidance-on-solarwinds-patch-a-15684

Chrome 修复了 Windows10 上的防病毒“文件锁定”错误

日期: 2021-01-03

等级: 中

来源: Ax Sharma

标签: ['Google Chrome', 'Windows 10', 'Antivirus', 'File Locking']

作为一种安全预防措施，通常防病毒程序会暂时锁定系统上新生成的文件，直到可以扫描这些文件并排除恶意活动。对此，google chrome 团队修复了一个相关的 bug，该 bug 使 windows10 上的防病毒程序能够锁定新创建的文件。修补这个漏洞意味着运行在 Windows 上的防病毒程序将不再阻止 Chrome 浏览器生成的新文件，比如书签。

详情

Google Chrome fixes antivirus 'file locking' bug on Windows 10

https://www.bleepingcomputer.com/news/security/google-chrome-fixes-antivirus-file-locking-bug-on-windows-10/

相关安全建议

1. 及时对系统及各个服务组件进行版本升级和补丁更新
2. 包括浏览器、邮件客户端、vpn、远程桌面等在内的个人应用程序，应及时更新到最新版本

四、 产品侧解决方案

（一）360 网络空间测绘系统

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

（二）360 安全分析响应平台

360 安全大脑的安全分析响应平台通过网络流量检测、多传感器数据融合关联分析手段，对该类漏洞的利用进行实时检测和阻断，请用户联系相关产品区域负责人或(shaoyulong#360.cn)获取对应产品。

（三）360 安全卫士

针对本次安全更新，Windows 用户可通过 360 安全卫士实现对应补丁安装，其他平台的用户可以根据修复建议列表中的产品更新版本对存在漏洞的产品进行更新。如有其他问题可联系相关产品负责人或（360safe-ent#360.cn）。

360CERT

附录 A 事件等级说明

高	
星级	★★★★/★★★★★
评定标准	1. 事件影响面十分广泛，受关注度高 2. 事件涉及的漏洞等级为严重/高危 3. 事件涉及机密/重要/核心数据， 4. 事件涉及数据量巨大 5. 事件涉及大型/常用厂商与组件 6. 事件涉及金额数目庞大/相关受害者损失高 7. 已知/潜在受害者数量庞大 8. 与日常生活/工作联系紧密
修复建议	建议在 3 个工作日内采取相关安全措施，并做好资产自测及预防工作

中	
星级	★★/★★★
危害结果	1. 事件影响面一般，受关注度中等 2. 事件涉及的漏洞等级为中危 3. 事件涉及数据机密性/重要性一般， 4. 事件涉及数据量中等 5. 事件涉及小型/常用厂商与组件 6. 事件涉及金额数目中等/相关受害者损失一般 7. 已知/潜在受害者数量中等 8. 与日常生活/工作联系一般
修复建议	建议在 7 个工作日内采取相关安全措施，并做好资产自测及预防工作

低

星级	★
危害结果	1. 事件影响面局限，受关注度低 2. 事件涉及的漏洞等级为低危 3. 事件涉及数据机密性/重要性低， 4. 事件涉及数据量低 5. 事件涉及小型/非常用厂商与组件 6. 事件涉及金额数目少/相关受害者损失低 7. 已知/潜在受害者数量少 8. 与日常生活/工作联系较小
修复建议	建议在 12 个工作日内采取相关安全措施，并做好资产自测及预防工作

360CERT

附录 B 事件类型说明

网络攻击事件	
描述：通过网络或其他技术手段，利用信息系统的配置缺陷、协议缺陷、程序缺陷或使用暴力攻击对终端设备实施攻击，并造成终端设备异常或对终端设备当前运行造成潜在危害的信息安全事件。	
网络扫描	对网络边界设备及终端进行批量信息探测，包括端口扫描、服务指纹探测、DNS 查询等
漏洞利用	黑客使用 0day 或 nday，对系统及服务进行攻击
web 攻击	黑客使用网络攻击技术，对 web 服务进行测试，包括 sql 注入、XSS、远程命令执行、恶意程序上传等
爆破事件	对网络设备及终端进暴力枚举及爆破，比如弱口令爆破、数据库爆破，系统路径爆破等
社工攻击	通过发送欺骗性垃圾邮件，或对目标发送构造的恶意信息，意图引诱目标给出敏感信息或者控制目标系统的攻击
DDos	使目标电脑的网络或系统资源耗尽，使服务暂时中断或停止，导致其正常用户无法访问。

360CERT

恶意程序事件	
描述：通过网络、便携式存储设备等途径散播的，故意对终端设备等造成隐私或机密数据外泄、系统损害、数据丢失等非使用预期故障及信息安全问题的程序	
后门攻击	利用软件系统、硬件系统设计过程中留下的后门或有害程序所设置的后门而对信息系统实施攻击的信息安全事件
勒索软件	勒索程序将受害者的电脑上锁，或系统性地加密受害者硬盘上的文件，并要求受害者缴纳赎金以取回对电脑的控制权
挖矿程序	程序占用终端设备资源进行虚拟货币赚取，导致服务器无法正常工作
僵尸网络	采用一种或多种传播手段，将大量主机感染 bot 程序（僵尸程序）病毒，从而在控制者和被感染主机之间所形成的可一对多控制的网络
蠕虫病毒	无须计算机使用者干预即可运行的独立程序，通过不停的取得网络中（存在漏洞的）计算机的部分或全部控制权来进行传播
其它病毒	除上述类别以外，其余未经许可，向终端设备植入的恶意程序

360CERT

数据安全事件	
描述：通过网络或其他技术手段，造成信息系统中的信息被篡改、假冒、泄漏、窃取等而导致的信息安全事件	
信息篡改	指未经授权，将信息系统中的信息更换为攻击者所提供的信息，而导致的信息安全事件，比如网页篡改、网页暗链等
信息假冒	通过假冒他人信息系统收发信息而导致的信息安全事件
信息泄漏	因误操作、软硬件缺陷或电磁泄漏等因素导致信息系统中的保密、敏感、个人隐私等信息暴露于未经授权者，而导致的信息安全事件
信息窃取	未经授权用户利用可能的技术手段，主动恶意获取信息系统中信息而导致的信息安全事件
信息丢失	指因误操作、人为蓄意或软硬件缺陷等因素导致信息系统中的信息丢失而导致的信息安全事件
信息内容	利用信息网络发布、传播危害国家安全、社会稳定和公共利益的内容的安全事件
其它信息破坏事件	指不能被包含在以上类别之中的信息破坏事件

其它安全事件	
描述：除开上述安全事件类型之外的事件	
设备设施故障	由于信息系统自身故障或外围保障设施故障，而导致的信息安全事件，以及人为地使用非技术手段，有意或无意的造成信息系统破坏，而导致的信息安全事件
灾害性事件	指由于不可抗力对信息系统造成物理破坏而导致的信息安全事件。
其它事件	不能归类于上述事件的安全事件

360CERT