安全事件周报

安全事件周报 (02.08-02.14)

360CERT
北京奇虎科技有限公司 | 2021-02-18

报告信息

报告名称	安全事件周报（02.08-02.14）		
报告类型	安全事件周报	报告编号	B6-2021-021801
报告版本	1.0	报告日期	2021-02-18
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	2021-02-18	360CERT	360CERT	撰写报告

目录

一、 事件概览

本周收录安全事件 12 项

话题集中在`勒索软件`、`漏洞修复`方面，涉及的组织有：`CD PROJEKT RED `、`SAP`、`Adobe`、`Yandex`等。代码仓库供应链攻击效果显著，代码上游安全管理需要重视。

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**
Cyberpunk 2077 恶意 mod 可接管用户主机	★★★★★
CD PROJEKT RED 游戏工作室遭勒索软件攻击	★★★★★
Egregor 勒索软件运营商在乌克兰被捕	★★★★
恶意 Android 应用劫持了数百万个设备	★★★★
数据安全	**等级**
Yandex 系统管理员出售用户电子邮件访问权限	★★★★
网络攻击	**等级**
黑客破坏奥尔兹马尔市供水设施	★★★★
PyPI，GitLab 处理垃圾邮件攻击	★★★★
研究人员通过供应链攻击威胁 35 家公司内部系统	★★★★
其他事件	**等级**
Adobe 修复了在野利用的严重漏洞	★★★★★
Google：我们的新工具使开源安全漏洞更容易被发现	★★★★
SAP Commerce 严重安全漏洞	★★★★
WordPress 插件漏洞使 10 万个站点遭受攻击	★★★★

三、 事件详情

(一) 恶意程序

Cyberpunk 2077 恶意 mod 可接管用户主机

日期: 2021-02-08

等级: 高

来源: Lawrence Abrams

标签: ['Cyberpunk 2077', 'Mod', 'ASLR', 'Vulnerability']

CD Projekt Red 发布了一个 Cyberpunk 2077 的修补程序，修复了一个代码执行漏洞，该漏洞可能被第三方数据文件修改和保存游戏文件所利用。攻击者利用缓冲区溢出漏洞，可以在计算机上执行命令，以及下载和安装恶意软件。若要避免此问题，请务必安装 Cyberpunk 2077 热补丁 1.12。

详情

Cyberpunk 2077 bug fixed that let malicious mods take over PCs

https://www.bleepingcomputer.com/news/security/cyberpunk-2077-bug-fixed-that-let-malicious-mods-take-over-pcs/

CD PROJEKT RED 游戏工作室遭勒索软件攻击

日期: 2021-02-09

等级: 高

来源: Sergiu Gatlan

标签: ['CD PROJEKT RED', 'Cyberpunk 2077', 'Ransomware']

cyberpunk2077 和 Witcher 三部曲背后的游戏开发工作室 CD PROJEKT RED 披露了一次影响其网络的勒索软件攻击。波兰游戏工作室在一份官方声明中说，攻击者破坏了内部网络，窃取了数据，并留下一张赎金纸条，攻击者声称，他们能够窃取 Cyberpunk 2077、Witcher 3、Gwent 的完整源代码，以及未发布的 Witcher 3 版本的源代码。CD PROJEKT RED 已经联系了相关部门，包括执法部门和个人数据保护办公室总裁，以及 IT 法医专家，以便全面调查这起事件。

详情

CD PROJEKT RED gaming studio hit by ransomware attack

https://www.bleepingcomputer.com/news/security/cd-projekt-red-gaming-studio-hit-by-ransomware-attack/

Egregor 勒索软件运营商在乌克兰被捕

日期: 2021-02-14

等级: 高

来源: Catalin Cimpanu

标签: ['Egregor', 'Ukraine', 'RaaS']

法国国际广播电台报道，Egregor 勒索软件卡特尔的成员已在乌克兰被逮捕。Egregor 团伙于 2020 年 9 月开始运作，以勒索软件即服务（RaaS）模式运作。他们依靠其他网络犯罪团伙策划对公司网络的入侵，并部署文件加密勒索软件。如果受害者支付了赎金，策划入侵的团伙将保留大部分资金，而 Egregor 团伙则从中分得一小部分。

详情

Egregor ransomware operators arrested in Ukraine

https://www.zdnet.com/article/egregor-ransomware-operators-arrested-in-ukraine/

恶意 Android 应用劫持了数百万个设备

日期: 2021-02-08

等级: 高

来源: Charlie Osborne

标签: ['Google Play', 'Lavabird']

Lavabird Ltd.的条形码扫描器是一款 Android 应用程序，多年来一直在谷歌官方应用程序库中提供下载。这款应用程序的安装量超过 1000 万次，它提供了二维码阅读器和条形码生成器。在 2020 年 12 月 4 日发布的一个软件更新后，应用程序变成了恶意软件，能够劫持多达 1000 万台设备，并投放大量的恶意广告。

详情

With one update, this malicious Android app hijacked millions of devices

https://www.zdnet.com/article/with-one-update-this-malicious-android-app-hijacked-10-million-devices/

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. 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
3. 条件允许的情况下，设置主机访问白名单
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

Yandex 系统管理员出售用户电子邮件访问权限

日期: 2021-02-12

等级: 高

来源: Ionut Ilascu

标签: ['Yandex', 'Sysadmin', 'Sold Access']

俄罗斯互联网和搜索公司 Yandex 宣布，该公司的一名系统管理员启用了对数千个用户邮箱的未经授权访问。该公司表示，管理人员这样做是为了"个人经济利益"。目前尚不清楚该员工何时开始向第三方提供未经授权的访问，但以这种方式泄露的收件箱总数达 4887 个。Yandex 将对管理访问程序进行更改，以提高用户数据的安全性。

详情

Yandex suffers data breach after sysadmin sold access to user emails

https://www.bleepingcomputer.com/news/security/yandex-suffers-data-breach-after-sysadmin-sold-access-to-user-emails/

相关安全建议

1. 注重内部员工安全培训
2. 管控内部员工数据使用规范，谨防数据泄露并及时做相关处理
3. 发生数据泄漏事件后，及时进行密码更改等相关安全措施

(三) 网络攻击

黑客破坏奥尔兹马尔市供水设施

日期: 2021-02-08

等级: 高

来源: Ionut Ilascu

标签: ['Oldsmar', 'TeamViewer', 'NaOH', 'Water Facility']

一名黑客通过 TeamViewer 远程进入了佛罗里达州奥尔兹马尔市的水处理系统，并试图将氢氧化钠（NaOH）的浓度（也称为碱液和苛性钠）提高到极其危险的水平。供水设施及时发现了浓度超标的危险情况，并做了应急处理，由于及时的干预，入城水质没有问题。水和废水处理是目前存在的关键基础设施中风险最大的领域之一，同时，许多水务公司都是小型实体，资源不足，因此很难构筑一个强大的安全防护。

详情

Hackers tried poisoning town after breaching its water facility

https://www.bleepingcomputer.com/news/security/hackers-tried-poisoning-town-after-breaching-its-water-facility/

PyPI，GitLab 处理垃圾邮件攻击

日期: 2021-02-09

等级: 高

来源: Catalin Cimpanu

标签: ['GitLab', 'PyPI', 'Spam Attacks']

PyPI 是 Python 编程语言的官方软件包存储库，也是一个拥有数万个 Python 库的网站。从 2021 年初开始，垃圾邮件运营商一直在滥用 Pypi 上的功能：任何人都可以在 PyPI 网站上创建条目，为根本不存在的 Python 库生成页面。由此，PyPI 库中充斥着 1 万多个垃圾广告页面，用于各种主题，从游戏到色情，从电影流媒体到赠品。2021 年二月初，PyPI 团队发表评论称，我们的管理员已经发现并开始解决垃圾邮件问题。同时，GitLab 发现了一个新的攻击，攻击者向数千个 GitLab 项目的订阅者发送了垃圾邮件，每个项目都会向帐户持有人发送一封电子邮件。就像 PyPI 上的垃圾邮件一样，这些评论也会将用户重定向到可疑网站。

详情

PyPI, GitLab dealing with spam attacks

https://www.zdnet.com/article/pypi-gitlab-dealing-with-spam-attacks/

研究人员通过供应链攻击威胁 35 家公司内部系统

日期: 2021-02-09

等级: 高

来源: Ax Sharma

标签: ['Supply Chain', 'PyPI', 'npm', 'RubyGems']

一名研究人员通过软件供应链攻击中，成功破解了微软、苹果、贝宝、Shopify、Netflix、Yelp、特斯拉和 Uber 等 35 家主要公司的内部系统。攻击包括将恶意软件上传到包括 PyPI、npm 和 RubyGems 在内的开源存储库，然后这些软件自动分发到公司内部应用程序的下游。这种特殊的供应链攻击更为复杂，因为它不需要受害者采取任何行动，而受害者会自动收到恶意软件包。由此，研究人员已经获得了超过 13 万美元的奖金。

详情

Researcher hacks Microsoft, Apple, more in novel supply chain attack

https://www.bleepingcomputer.com/news/security/researcher-hacks-microsoft-apple-more-in-novel-supply-chain-attack/

相关安全建议

1. 软硬件提供商要提升自我防护能力，保障供应链的安全
2. 条件允许的情况下，设置主机访问白名单
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. 积极开展外网渗透测试工作，提前发现系统问题

(四) 其他事件

Adobe 修复了在野利用的严重漏洞

日期: 2021-02-09

等级: 高

来源: Lawrence Abrams

标签: ['Adobe', 'Adobe Reader', 'Command Execution']

Adobe 已经发布了安全更新，解决了 Adobe Reader 中的本地任意代码执行漏洞--`CVE-2021-21017`，攻击者通过此漏洞，在目标上打开或者诱导目标用户打开恶意文档，可以直接接管目标机器。请尽快下载并更新 Adobe Reader 到最新版本。

链接：
- https://helpx.adobe.com/security/products/acrobat/apsb21-09.html
- https://get.adobe.com/reader

详情

Adobe fixes critical Reader vulnerability exploited in the wild

https://www.bleepingcomputer.com/news/security/adobe-fixes-critical-reader-vulnerability-exploited-in-the-wild/

Google：我们的新工具使开源安全漏洞更容易被发现

日期: 2021-02-08

等级: 高

来源: Liam Tung

标签: ['Google', 'OSV', 'Vulnerability Databases']

Google 已启动了开放源代码漏洞（OSV）网站，该网站提供了一个漏洞数据库，可帮助您对开放源代码项目中的错误进行分类，并帮助开放源代码的维护者和使用者。同时，它还为开源社区提出了一个框架，以判断哪些项目应被视为重要项目，并对为这些项目做出贡献的开发人员制定更严格的规定。

详情

Google: Our new tool makes open-source security bugs easier to spot

https://www.zdnet.com/article/google-our-new-tool-makes-open-source-security-bugs-easier-to-spot/

SAP Commerce 严重安全漏洞

日期: 2021-02-10

等级: 高

来源: Lindsey O'Donnell

标签: ['SAP', 'SAP Commerce', 'RCE']

SAP 警告称，其针对电子商务业务的 SAP Commerce 平台存在严重漏洞。如果被利用，攻击者可直接执行远程代码。该漏洞（CVE-2021-21477）影响 SAP Commerce 版本 1808、1811、1905、2005 和 2011。CVSS 评分：9.9。

详情

SAP Commerce Critical Security Bug Allows RCE

https://threatpost.com/sap-commerce-critical-security-bug/163822/

WordPress 插件漏洞使 10 万个站点遭受攻击

日期: 2021-02-11

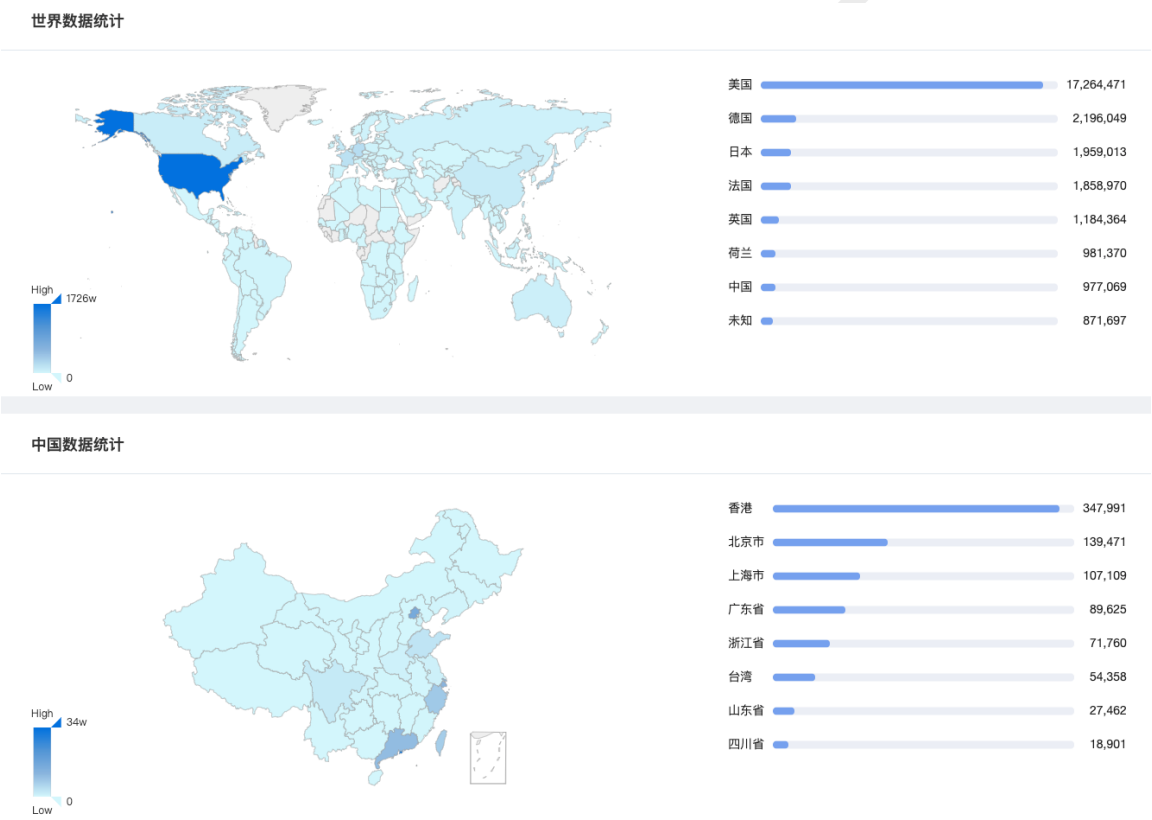
等级: 高

来源: Sergiu Gatlan

标签: ['Responsive Menu', 'WordPress']

Wordpress 中的插件--Responsive Menu 存在任意文件上传和远程代码执行漏洞，利用此漏洞的攻击者可直接接管站点。该插件旨在帮助管理员创建 W3C 兼容且可移动的负责站点菜单，安装量超过 10 万。请使用此插件的用户务必在管理页面中尽快更新该插件。

目前 wordpress 的具体分布如下图，数据来自于 360 QUAKE



详情

Buggy WordPress plugin exposes 100K sites to takeover attacks

https://www.bleepingcomputer.com/news/security/buggy-wordpress-plugin-exposes-100k-sites-to-takeover-attacks/

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）。

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

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。

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

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