安全事件周报

安全事件周报 (08.02-08.08)

360CERT

360CERT
北京奇虎科技有限公司

报告信息

报告名称	安全事件周报 (08.02-08.08)		
报告类型	安全事件周报	报告编号	B6-2021-080901
报告版本	1	报告日期	2021-08-09
报告作者	360CERT	联系方式	g-cert-report@360.cn
提供方	北京鸿腾智能科技有限公司-360CERT		
接收方			

报告修订记录

报告版本	日期	修订	审核	描述
1	2021-08-09	360CERT	360CERT	撰写报告

目录

360CERT

360CERT

1 事件导览

本周收录安全热点6项，话题集中在勒索软件、网络攻击方面，涉及的组织有：One MoreLead、Microsoft、技嘉等。勒索软件肆虐，各厂商注意防护。对此，360CERT建议使用360安全卫士进行病毒检测、使用360安全分析响应平台进行威胁流量检测，使用360城市级网络安全监测服务QUAKE进行资产测绘，做好资产自查以及预防工作，以免遭受黑客攻击。

360CERT

2 事件目录

恶意程序
FBI 发现了 100 多个活跃的勒索软件变种
硬件厂商技嘉遭勒索软件攻击
破坏美国最大燃油管道的黑客团伙卷土重来

数据安全
vpnMentor 报告显示 6300 万美国用户的信息遭泄露

其它事件
PTS 系统中的 PwnedPiper 漏洞影响了 80% 的美国医院
工业控制设备中广泛使用的嵌入式 TCP/IP 协议栈存在严重漏洞

360CERT

3 恶意程序

3.1 FBI 发现了 100 多个活跃的勒索软件变种

1 日期：2021 年 08 月 02 日
2 等级：高
3 来源：heimdalsecurity
4 标签：fbi, Colony Pipe, kaseya, Ransomware Variants
5 行业：跨行业事件
6 涉及组织：fbi

联邦调查局 (FBI) 发布了一份官方声明，警告说 100 多种活跃的勒索软件变种正忙于对美国企业、学校和其他组织发起攻击。

该声明是在几次备受瞩目的勒索软件攻击的背景下发表的，其中包括对 ColonyPipe 和 kaseya 的攻击。根据该局的说法，随着"双重勒索"攻击的增加，网络犯罪分子增强了他们增大勒索软件攻击规模和影响。

详情

FBI Finds Over 100 Active Ransomware Variants

3.2 中国台湾硬件厂商技嘉遭勒索软件攻击

1 日期：2021 年 08 月 07 日
2 等级：高
3 作者：cnBeta.COM
4 标签：Gigabyte, RansomExx
5 行业：制造业

技嘉科技股份有限公司（Gigabyte）是中国台湾一家以制造及贩售电子科技硬件为主的民营企业，于 8 月 3 号晚遭到勒索软件攻击。黑客威胁称如果公司不支付赎金，将公开 112GB 的公司内部数据。技嘉在公告中表示，公司于 8 月 3 号晚上遭到勒索软件攻击，但没有对生产系统产生影响，因为攻击的目标是位于总部的少量内部服务器。技嘉表示由于安全团队的迅速行动，服务器已从备份中恢复并重新上线，但事件远未结束。援引外媒 TheRecord 报道，勒索软件团伙 RansomExx 对本次攻击负责。

详情

技嘉遭勒索软件攻击

3.3 破坏美国最大燃油管道的黑客团伙卷土重来

```
日期：2021 年 08 月 08 日
等级：高
来源：cnbeta
标签：DarkSide, BlackMatter
行业：跨行业事件
```

在 2021 年 5 月，黑客团伙 DarkSide 导致美国“输油大动脉”一度瘫痪，甚至让宣布进入国家紧急状态，也因此声名大噪。在成功获得了赎金后，迫于多方压力最终 DarkSide 宣布解散。

根据网络安全公司 RecordedFuture 的说法，新成立的黑客团伙名为黑物质集团(BlackMatterGroup)，该组织声称其已经成功融合了 DarkSide 和勒索软件“REvil”和“Lockbit”的最佳功能。

详情

搞瘫美国最大燃油管道的黑客软件卷土重来

3.4 ** 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. 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. 各主机安装 EDR 产品，及时检测威胁
6. 注重内部员工安全培训
7. 不轻信网络消息，不浏览不良网站、不随意打开邮件附件，不随意运行可执行程序
8. 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

360CERT

4 数据安全

4.1 vpnMentor 报告显示 6300 万美国用户的信息遭泄露

1 日期：2021 年 08 月 06 日
2 等级：高
3 作者：cnBeta.COM
4 标签：VPNMentor，OneMoreLead
5 行业：信息传输、软件和信息技术服务业
6 涉及组织：OneMoreLead，VPNMentor

据外媒报道，VPNMentor 发现了一起重大数据泄露事件，估计有 6300 万美国公民的信息被泄露。这个数据库属于 OneMoreLead，它被指控将用户信息（工作地点、电子邮件地址和姓名）储存在一个没有保护的数据库中。

详情

vpnMentor 报告显示 6300 万美国用户的信息遭泄露

4.2 ** 相关安全建议 **

1. 及时备份数据并确保数据安全
2. 合理设置服务器端各种文件的访问权限
3. 严格控制数据访问权限

4. 及时检查并删除外泄敏感数据
5. 发生数据泄漏事件后，及时进行密码更改等相关安全措施
6. 强烈建议数据库等服务放置在外网无法访问的位置，若必须放在公网，务必实施严格的访问控制措施

360CERT

5 其它事件

5.1 PTS 系统中的 PwnedPiper 漏洞影响了 80% 的美国医院

日期：2021 年 08 月 02 日
等级：高
作者：Pierluigi Paganini
标签：pwnedpiper, US hospitals
行业：卫生和社会工作

来自网络安全 armis 的研究人员披露了 9 个漏洞，这些漏洞统称为 pwnedpiper，可被利用来对广泛使用的气动管系统 (pts) 进行多次攻击。swisslogpts 系统用于医院，通过气动管网络实现整个建筑的物流和材料运输自动化。该漏洞影响了 swisslogHealthcare 制造的 translogicpts 系统，该系统安装在北美约 80% 的医院中。

5.1.1 涉及漏洞

5.1.2 cve-2021-37161

链接: https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2021-37161

5.1.3 cve-2021-37162

链接: https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2021-37162

5.1.4 cve-2021-37163

链接: https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2021-37163

5.1.5 cve-2021-37164

链接: https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2021-37164

5.1.6 cve-2021-37165

链接: https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2021-37165

5.1.7 cve-2021-37166

链接: https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2021-37166

5.1.8 cve-2021-37167

链接: https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2021-37167

5.1.9 cve-2021-37160

链接: https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2021-37160

360CERT

5.1.10 IOC

Ip

- 7.2.5.7

详情

PwnedPiper flaws in PTS systems affect 80% of major US hospitals

5.2 工业控制设备中广泛使用的嵌入式 TCP/IP 协议栈存在严重漏洞

日期：2021 年 08 月 04 日
等级：高
作者：Ravie Lakshmanan
标签：Industrial Control Devices, TCP/IP Stack, vulnerabilities
行业：电力、热力、燃气及水生产和供应业

网络安全研究人员在 8 月 4 日披露了 14 个影响常用 tcp/ip 堆栈的漏洞，该堆栈用于由不少于 200 家供应商制造并部署在制造工厂、发电、水处理和基础设施部门的数百万个操作技术 (ot) 设备中使用。
漏洞存在于 nichestack（又名 interniche 堆栈，是一种用于嵌入式系统的闭源 tcp/ip 堆栈），利用漏洞攻击者能够实现远程代码执行、拒绝服务、信息泄漏、tcp 欺骗，甚至 dns 缓存中毒。

5.2.1 涉及漏洞

5.2.2 cve-2020-25928

链接: https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2020-25928

5.2.3 cve-2021-31226

链接: https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2021-31226

5.2.4 cve-2020-25927

链接: https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2020-25927

5.2.5 cve-2020-25767

链接: https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2020-25767

5.2.6 cve-2021-31227

链接: https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2021-31227

5.2.7 cve-2021-31400

链接: https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2021-31400

5.2.8 cve-2021-31401

链接: https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2021-31401

360CERT

5.2.9 cve-2020-35683

链接: https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2020-35683

5.2.10 cve-2020-35684

链接: https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2020-35684

5.2.11 cve-2020-35685

链接: https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2020-35685

5.2.12 cve-2021-27565

链接: https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2021-27565

5.2.13 cve-2021-36762

链接: https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2021-36762

5.2.14 cve-2020-25926

链接: https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2020-25926

5.2.15 cve-2021-31228

链接: https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2021-31228

详情

Critical Flaws Affect Embedded TCP/IP Stack Widely Used in Industrial Control Devices

5.3 ** 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

360CERT

6 时间线

2021-08-09 360CERT 发布安全事件周报

360CERT

A 产品侧解决方案

若想了解更多信息或有相关业务需求，可移步至http://360.net

A.1 360 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。

A.2 360 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，对网络攻击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。

A.3 360 安全卫士

针对以上安全事件，360cert 建议广大用户使用 360 安全卫士定期对设备进行安全检测，以做好资产自查以及防护工作。