北京师范大学网络信息安全通告

2020 年 9 月报告

北京师范大学信息网络中心

2020 年 10 月

信息安全漏洞周报

2020年　9月　　1 周

CNNVD　　2020 年 9 月 6 日

根据国家信息安全漏洞库（CNNVD）统计，本周（2020 年 08 月 31 日至 2020 年 09 月 06 日）安全漏洞情况如下：

公开漏洞情况

本周 CNNVD 采集安全漏洞 353 个，与上周（264 个）相比增加了 33.71%。

接报漏洞情况

本周 CNNVD 接报漏洞 1274 个，其中信息技术产品漏洞（通用型漏洞）50 个，网络信息系统漏洞（事件型漏洞）1224 个。

一、公开漏洞情况

根据国家信息安全漏洞库（CNNVD）统计，本周新增安全漏洞 353 个，漏洞新增数量有所上升。从厂商分布来看 GitLab 公司新增漏洞最多，有 19 个；从漏洞类型来看，跨站脚本类的安全漏洞占比最大，达到 15.86%。新增漏洞中，超危漏洞 42 个，高危漏洞 91 个，中危漏洞 215 个，低危漏洞 5 个。相应修复率分别为 80.95%、69.23%、70.70%和 100.00%。根据补丁信息统计，合计 254 个漏洞已有修复补丁发布，整体修复率为 71.95%。

（一） 安全漏洞增长数量情况

本周 CNNVD 采集安全漏洞 353 与上周（264 个）相比增多了 33.71%。

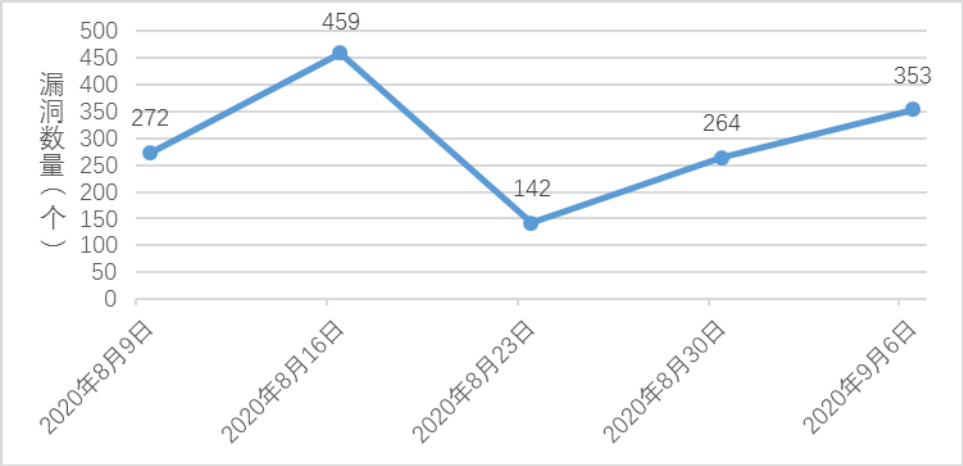

图 1 近五周漏洞新增数量统计图

（二） 安全漏洞分布情况

从厂商分布来看，GitLab 公司新增漏洞最多，有 19 个。各厂商漏洞数量分布如表 1 所示。

表 1 新增安全漏洞排名前五厂商统计表

序号	厂商名称	漏洞数量（个）	所占比例
1	GitLab	19	5.38%
2	IBM	17	4.82%
3	Cisco	17	4.82%
4	CloudBees	14	3.97%
5	Google	13	3.68%

本周国内厂商漏洞 13 个，Huawei 公司漏洞数量最多，有 3 个。国内厂商漏洞整体修复率为 90.91%。请受影响用户关注厂商修复情况，及时下载补丁修复漏洞。

从漏洞类型来看，跨站脚本类的安全漏洞占比最大，达到 15.86%。漏洞类型统计如表 2 所示。

表 2 漏洞类型统计表

序号	漏洞类型	漏洞数量（个）	所占比例
1	跨站脚本	56	15.86%
2	SQL 注入	31	8.78%
3	输入验证错误	25	7.08%
4	信息泄露	11	3.12%
5	路径遍历	5	1.42%
6	代码问题	5	1.42%
7	代码注入	5	1.42%
8	跨站请求伪造	4	1.13%
9	缓冲区错误	3	0.85%
10	命令注入	2	0.57%
11	权限许可和访问控制问题	2	0.57%
12	操作系统命令注入	1	0.28%
13	加密问题	1	0.28%
14	访问控制错误	1	0.28%
15	信任管理问题	1	0.28%
16	注入	1	0.28%
17	数据伪造问题	1	0.28%
18	日志信息泄露	1	0.28%
19	后置链接	1	0.28%
20	其他	153	43.34%

（三） 安全漏洞危害等级与修复情况

本周共发布超危漏洞 42 个，高危漏洞 91 个，中危漏洞 215 个，低危漏洞 5 个。相应修复率分别为 80.95%、69.23%、70.70%和 100.00%。根据补丁信息统计，合计 254 个漏洞已有修复补丁发布，整体修复率为 71.95%。详细情况如表 3 所示。

表 3 漏洞危害等级与修复情况

序号	危害等级	漏洞数量（个）	修复数量（个）	修复率
1	超危	42	34	80.95%
2	高危	91	63	69.23%
3	中危	215	152	70.70%
4	低危	5	5	100.00%
合计		353	254	71.95%

（四） 本周重要漏洞实例

本期重要漏洞实例如表 4 所示。

表 4 本期重要漏洞实例

序号	漏洞类型	漏洞编号	厂商	漏洞实例	是否修复	危害等级
1	其他	CNNVD-202008-1494	Google	Android 安全漏洞	是	超危
2	跨站请求伪造	CNNVD-202009-028	CloudBees	CloudBees Jenkins CSRF 漏洞	是	高危
3	其他	CNNVD-202009-295	IBM	IBM Aspera Connect 安全漏洞	是	高危

1. Android 安全漏洞（CNNVD-202008-1494）

Android 是美国谷歌（Google）和开放手持设备联盟（简称 OHA）的一套以 Linux 为基础的开源操作系统。Framework 是其中的一个 Android 框架组件。System 是其中的一个系统组件。Broadcom

Bluetooth 是其中的一个蓝牙组件。Wi-Fi 是其中的一个无线上网组件。USB driver 是其中的一个通用串行总线（USB）驱动程序。VPN 是其中的一个 VPN（虚拟专用网络）组件。Bluetooth 是其中的一个蓝牙组件。Email 是其中的一个电子邮件组件。

Android OS 9 and 10 中的 LG mobile 设备存在安全漏洞，攻击者利用此漏洞可以绕过权限限制。

目前厂商已发布升级补丁以修复漏洞，详情请关注厂商主页：

https://lgsecurity.lge.com/

2. CloudBees Jenkins CSRF 漏洞（CNNVD-202009-028）

CloudBees Jenkins（Hudson Labs）是美国 CloudBees 公司的一套基于 Java 开发的持续集成工具。该产品主要用于监控持续的软件版本发布/测试项目和一些定时执行的任务。LTS 是 CloudBeesJenkins 的一个长期支持版本。

Jenkins database Plugin 1.6 及之前版本存在 CSRF 漏洞，该漏洞源于 WEB 应用未充分验证请求是否来自可信用户。攻击者可利用该漏洞通过受影响客户端向服务器发送非预期的请求。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://vigilance.fr/vulnerabilite/Jenkins-Plugins-multiples-vulnerabilites-33205

3. IBM Aspera Connect 安全漏洞（CNNVD-202009-295）

IBM Aspera 是美国 IBM 公司的一套基于 IBM FASP 协议构建的快速文件传输和流解决方案。

IBM Aspera Connect 3.9.9 版本存在安全漏洞，该漏洞源于动态链接库加载不正确，攻击者可以利用此漏洞诱使受害者打开特制的.DLL 文件，从而执行任意代码。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://www.ibm.com/support/pages/node/6326537

二、接报漏洞情况

本周 CNNVD 接报漏洞 1274 个，其中信息技术产品漏洞（通用型漏洞）50 个，网络信息系统漏洞（事件型漏洞）1224 个。

表 5 本周漏洞报送情况

序号	报送单位	漏洞总量
1	上海斗象信息科技有限公司	648
2	网神信息技术（北京）股份有限公司	356
3	内蒙古奥创科技有限公司	94
4	北京奇虎科技有限公司	37
5	杭州海康威视数字技术股份有限公司	36
6	西安交大捷普网络科技有限公司	24
7	北京山石网科信息技术有限公司	11
8	北京数字观星科技有限公司	10
9	美团安全	10
10	湖南匡安网络技术有限公司	8
11	个人	7
12	中国电信集团系统集成有限责任公司	6

13	新华三技术有限公司	5
14	安全邦（北京）信息技术有限公司	5
15	重庆梦之想科技有限公司	4
16	苏州极光无限信息技术有限公司	2
17	上海安识网络科技有限公司	2
18	阿里安全	1
19	安徽长泰信息安全服务有限公司	1
20	北京网御星云信息技术有限公司	1
21	国网山西省电力公司电力科学研究院	1
22	江西神舟信息安全评估中心有限公司	1
23	上海市信息安全测评中心	1
24	深信服科技股份有限公司	1
25	亚信科技（成都）有限公司	1
26	中国电信集团系统集成有限责任公司云计算安全与服务事业部	1
报送总计		1274

三、接报漏洞预警情况

本周 CNNVD 接报漏洞预警 31 个。

序号	报送单位	漏洞总量
1	杭州迪普科技有限公司	15
2	北京知道创宇信息技术股份有限公司	4
3	北京华云安信息技术有限公司	4
4	北京启明星辰信息安全技术有限公司	2
5	网神信息技术（北京）股份有限公司	1

6	新华三技术有限公司	1
7	杭州安恒信息技术股份有限公司	1
8	深信服科技股份有限公司	1
9	北京山石网科信息技术有限公司	1
10	内蒙古洞明科技有限公司	1
报送总计		31

信息安全漏洞周报

2020 年 9月 2 周

CNNVD **2020 年 9 月 13 日**

根据国家信息安全漏洞库（CNNVD）统计，本周（2020 年 09 月 07 日至 2020 年 09 月 13 日）安全漏洞情况如下：

公开漏洞情况

本周 CNNVD 采集安全漏洞 410 个，与上周（353 个）相比增加了 16.15%。

接报漏洞情况

本周 CNNVD 接报漏洞 1231 个，其中信息技术产品漏洞（通用型漏洞）103 个，网络信息系统漏洞（事件型漏洞）1128 个。

重大漏洞预警

微软多个安全漏洞：包括多款 Microsoft Exchange server 安全漏洞（CNNVD-202009-374、CVE-2020-16875）、Microsoft SharePoint 安全漏洞（CNNVD-202009-384、CVE-2020-1452）等。成功利用上述漏洞的攻击者可以在目标系统上执行任意代码、获取用户数据，提升权限等。微软多个产品和系统受漏洞影响。目前，微软官方已经发布漏洞修复补丁，建议用户及时确认是否受到漏洞影响，尽快采取修补措施。

一、公开漏洞情况

根据国家信息安全漏洞库（CNNVD）统计，本周新增安全漏洞 410 个，漏洞新增数量有所上升。从厂商分布来看 Microsoft 公司新增漏洞最多，有 121 个；从漏洞类型来看，输入验证错误类的安全漏洞占比最大，达到 10.00%。新增漏洞中，超危漏洞 23 个，高危漏洞 121 个，中危漏洞 254 个，低危漏洞 12 个。相应修复率分别为 95.65%、99.17%、94.49%和 100.00%。根据补丁信息统计，合计 394 个漏洞已有修复补丁发布，整体修复率为 96.10%。

（一） 安全漏洞增长数量情况

本周 CNNVD 采集安全漏洞 410 与上周（353 个）相比增多了 16.15%。

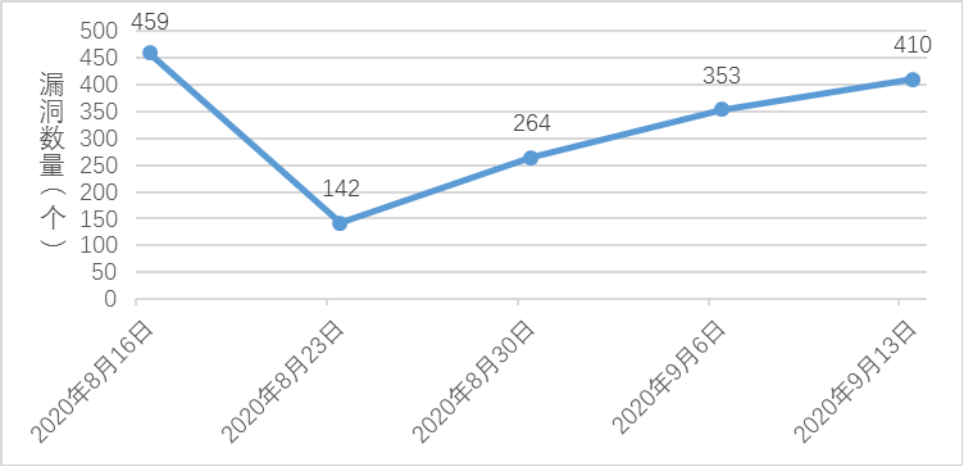

图 1 近五周漏洞新增数量统计图

（二） 安全漏洞分布情况

从厂商分布来看，Microsoft 公司新增漏洞最多，有 121 个。各厂商漏洞数量分布如表 1 所示。

表 1 新增安全漏洞排名前五厂商统计表

序号	厂商名称	漏洞数量（个）	所占比例
1	Microsoft	121	29.51%
2	SAP	52	12.68%
3	Google	45	10.98%
4	Adobe	18	4.39%
5	Siemens	10	2.44%

本周国内厂商漏洞 6 个，小米公司漏洞数量最多，有 2 个。国内厂商漏洞整体修复率为 100.00%。请受影响用户关注厂商修复情况，及时下载补丁修复漏洞。

从漏洞类型来看，输入验证错误类的安全漏洞占比最大，达到 10.00%。漏洞类型统计如表 2 所示。

表 2 漏洞类型统计表

序号	漏洞类型	漏洞数量（个）	所占比例
1	输入验证错误	41	10.00%
2	跨站脚本	25	6.10%
3	缓冲区错误	19	4.63%
4	跨站请求伪造	9	2.20%
5	信息泄露	9	2.20%
6	代码问题	7	1.71%
7	授权问题	6	1.46%
8	SQL 注入	5	1.22%
9	资源管理错误	4	0.98%
10	访问控制错误	3	0.73%
11	日志信息泄露	3	0.73%
12	操作系统命令注入	2	0.49%
13	代码注入	2	0.49%
14	后置链接	2	0.49%
15	配置错误	2	0.49%
16	命令注入	1	0.24%
17	加密问题	1	0.24%
18	其他	208	50.73%

（三） 安全漏洞危害等级与修复情况

本周共发布超危漏洞 23 个，高危漏洞 121 个，中危漏洞 254 个，低危漏洞 12 个。相应修复率分别为 95.65%、99.17%、94.49%和 100.00%。根据补丁信息统计，合计 394 个漏洞已有修复补丁发布，整体修复率为 96.10%。详细情况如表 3 所示。

表 3 漏洞危害等级与修复情况

序号	危害等级	漏洞数量（个）	修复数量（个）	修复率
1	超危	23	22	95.65%
2	高危	121	120	99.17%
3	中危	254	240	94.49%
4	低危	12	12	100.00%
合计		410	394	96.10%

（四） 本周重要漏洞实例

本期重要漏洞实例如表 4 所示。

表 4 本期重要漏洞实例

序号	漏洞类型	漏洞编号	厂商	漏洞实例	是否修复	危害等级
1	其他	CNNVD-202009-374	Microsoft	Microsoft Exchange server 安全漏洞	是	超危
2	其他	CNNVD-202009-516	Google	Google Chrome 安全漏洞	是	高危
3	特权升级	CNNVD-202009-664	Linux	Linux kernel 特权升级漏洞	是	高危

1. Microsoft Exchange server 安全漏洞（CNNVD-202009-374）

Microsoft Exchange Server 是美国微软（Microsoft）公司的一套电子邮件服务程序。它提供邮件存取、储存、转发，语音邮件，邮件过滤筛选等功能。

Microsoft Exchange server 中存在远程代码执行漏洞，该漏洞源于 cmdlet 参数的验证不当，攻击者可利用该漏洞在系统用户上下文中运行任意代码。

目前厂商已发布升级补丁以修复漏洞，详情请关注厂商主页：

https://portal.msrc.microsoft.com/en-us/security-guidance

2. Google Chrome 安全漏洞（CNNVD-202009-516）

Google Chrome 是美国谷歌（Google）公司的一款 Web 浏览器。

Google Chrome 存在安全漏洞，该漏洞源于网络中的策略执行不足，攻击者可以利用此漏洞绕过安全限制。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://chromereleases.googleblog.com/2020/09/stable-channel-update-for-desktop.html

3. Linux kernel 特权升级漏洞（CNNVD-202009-664）

Linux kernel 是美国 Linux 基金会发布的开源操作系统 Linux 所使用的内核。

Linux kernel 中存在特权升级漏洞。该漏洞源于网络系统或产品中缺少身份验证措施或身份验证强度不足。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://www.openwall.com/lists/oss-security/2020/09/10/4

二、接报漏洞情况

本周 CNNVD 接报漏洞 1231 个，其中信息技术产品漏洞（通用型漏洞）103 个，网络信息系统漏洞（事件型漏洞）1128 个。

表 5 本周漏洞报送情况

序号	报送单位	漏洞总量
1	上海斗象信息科技有限公司	521
2	网神信息技术（北京）股份有限公司	471
3	北京华云安信息技术有限公司	71
4	远江盛邦(北京)网络安全科技股份有限公司	20
5	浙江国利网安科技有限公司	20
6	中国电子科技网络信息安全有限公司	18
7	北京微步在线科技有限公司	17
8	北京天地和兴科技有限公司	17
9	蚂蚁集团-天穹实验室	13
10	绿盟科技集团股份有限公司	11
11	北京天融信网络安全技术有限公司	10
12	北京数字观星科技有限公司	10
13	北京安华金和科技有限公司	5
14	安徽长泰信息安全服务有限公司	4
15	浙江国利网安科技有限公司	3
16	安徽锋刃信息科技有限公司	3
17	北京安信天行科技有限公司	3
18	重庆梦之想科技有限公司	3

19	北京智游网安科技有限公司	2
20	内蒙古洞明科技有限公司	2
21	北京天融信网络安全技术有限公司	1
22	国网山西省电力公司电力科学研究院	1
23	美团安全	1
24	天津市兴先道科技有限公司	1
25	信息工程大学	1
26	浙江东安检测技术有限公司	1
27	个人	1
报送总计		1231

三、接报漏洞预警情况

本周 CNNVD 接报漏洞预警 60 个。

1	报送单位	漏洞总量
1	杭州迪普科技有限公司	14
2	内蒙古奥创科技有限公司	10
3	恒安嘉新（北京）科技股份公司	6
4	北京华顺信安科技有限公司	6
5	深信服科技股份有限公司	5
6	网神信息技术（北京）股份有限公司	4
7	北京知道创宇信息技术股份有限公司	3
8	北京华云安信息技术有限公司	3
9	北京顶象技术有限公司 洞见安全实验室	2
10	北京山石网科信息技术有限公司	2

11	杭州安恒信息技术股份有限公司	2
12	北京启明星辰信息安全技术有限公司	1
13	北京神州绿盟科技有限公司	1
14	北京天融信网络安全技术有限公司	1
报送总计		60

四、重大漏洞预警

微软多个安全漏洞预警

近日，微软官方发布了多个安全漏洞的公告，包括多款Microsoft Exchange server 安全漏洞（CNNVD-202009-374、CVE-2020-16875）、Microsoft SharePoint 安全漏洞（CNNVD-202009-384、CVE-2020-1452）、Microsoft Word 安全漏洞（CNNVD-202009-390、CVE-2020-1218）等多个漏洞。成功利用上述漏洞的攻击者可以在目标系统上执行任意代码、获取用户数据，提升权限等。微软多个产品和系统受漏洞影响。目前，微软官方已经发布漏洞修复补丁，建议用户及时确认是否受到漏洞影响，尽快采取修补措施。

.漏洞介绍

2020 年 9 月 9 日，微软发布了 2020 年 9 月份安全更新，共 129 个漏洞的补丁程序，CNNVD 对这些漏洞进行了收录。本次更新涵盖了 Windows 操作系统、IE/Edge 浏览器、ChakraCore、SQL Server、Office 组件及 Web Apps、Exchange 服务器、Windows Defender 等多个 Windows 平台下应用软件和组件。微软多个产品和系统版本受漏洞影响，具体

影响范围可访问微软官方网站 https://portal.msrc.microsoft.com/zh-cn/security-guidance 查询，其中部分重要漏洞详情如下：

1、Microsoft Exchange server 安全漏洞（CNNVD-202009-374、CVE-2020-16875）

漏洞简介：Microsoft Exchange server 中存在远程代码执行漏洞，该漏洞源于 cmdlet 参数的验证不当，攻击者可利用该漏洞在系统用户上下文中运行任意代码。

2、Microsoft SharePoint 安全漏洞（CNNVD-202009-384、CVE-2020-1452）（CNNVD-202009-382、CVE-2020-1460）（CNNVD-202009-393、CVE-2020-1200）（CNNVD-202009-391、CVE-2020-1210）（CNNVD-202009-376、CVE-2020-1576）

漏洞简介：Microsoft SharePoint 中存在安全漏洞。该漏洞源于网络系统或产品中缺少身份验证措施或身份验证强度不足。攻击者可以利用该漏洞获得与当前用户相同的用户权限。

3、Microsoft Word 安全漏洞（CNNVD-202009-390、CVE-2020-1218）（CNNVD-202009-386、CVE-2020-1338）

漏洞简介：Microsoft Word 中存在资源管理漏洞。该漏洞源于软件无法正确处理内存中的对象。

4、Microsoft Excel 安全漏洞（CNNVD-202009-371、CVE-2020-1594）（CNNVD-202009-387、CVE-2020-1335）（CNNVD-202009-372、CVE-2020-1332）（CNNVD-202009-373、CVE-2020-1193）

漏洞简介：Microsoft Excel 中存在授权问题漏洞。该漏洞源于网络系统或产品中缺少身份验证措施或身份验证强度不足。攻击者可以利用该漏洞获得与当前用户相同的用户权限。

5、Microsoft Dynamics 365 和 Microsoft Dynamics 安全漏洞（ CNNVD-202009-490、 CVE-2020-16862）（CNNVD-202009-467、CVE-2020-16860）

漏洞简介：Microsoft Dynamics 365 (on-premises) 存在远程代码执行漏洞。该漏洞允许攻击者向易受攻击的 Dynamics 服务器发送特制的请求，从而导致攻击者可以在 SQL 服务帐户中运行任意代码。

6、Microsoft Windows 安全漏洞（CNNVD-202009-412、CVE-2020-1319）（ CNNVD-202009-428、CVE-2020-1129)

漏洞简介：Microsoft Windows Codecs 存在安全漏洞，该漏洞源于处理内存中的对象，存在远程执行代码漏洞。攻击者可利用该漏洞获取信息，从而进一步入侵用户系统。

7、Windows Media 安全漏洞（CNNVD-202009-407、 CVE-2020-1508）（CNNVD-202009-399、CVE-2020-1593）

漏洞简介：Windows Media 中存在安全漏洞。该漏洞源于 Windows Media 音频解码器不正确地处理对象，攻击者可利用该漏洞获取用户信息。

8、Microsoft Windows Jet 数据库安全漏洞（ CNNVD-202009-434、CVE-2020-1074)（CNNVD-202009-438、CVE-2020-1039）

漏洞简介：Windows Jet 数据库存在安全漏洞，该漏洞源于不正确地披露其内存中的内容。攻击者可利用该漏洞执行任意代码。

9、Windows GDI 安全漏洞（ CNNVD-202009-415、CVE-2020-1285）

漏洞简介：Windows GDI 中存在安全漏洞。攻击者可借助该漏洞控制受影响的系统，可以安装程序；查看、更改或删除数据；或者创建拥有完全用户权限的新帐户。

10、Microsoft 浏览器安全漏洞（ CNNVD-202009-368、CVE-2020-0878)

漏洞简介：Microsoft 浏览器存在安全漏洞，该漏洞允许攻击者以执行任意代码的方式损坏内存，并可以获得与当前用户相同的用户权限。

11、Microsoft COM 安全漏洞(CNNVD-202009-452、CVE-2020-0922)

漏洞简介：Microsoft COM 存在远程代码执行漏洞，该漏洞源于外部输入数据构造代码段的过程中，网络系统或产品未正确过滤其中的特殊元素。攻击者可利用该漏洞生成非法的代码段，修改网络系统或组件的预期的执行控制流。

.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 Exchange server 安全漏洞（ CNNVD-202009-374、 CVE-2020-16875）	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-16875
2	Microsoft SharePoint 安全漏洞（ CNNVD-202009-384 、 CVE-2020-1452 ）（ CNNVD-202009-382 、 CVE-2020-1460 ）	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-1452 https://portal.msrc.microsoft.com/zh-CN/security-guidance

	（CNNVD-202009-393、CVE-2020-1200）（CNNVD-202009-391、CVE-2020-1210）（CNNVD-202009-376、CVE-2020-1576）	/advisory/CVE-2020-1460 https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-1200 https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-1210 https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-1576
3	Microsoft Word 安全漏洞（CNNVD-202009-390、CVE-2020-1218）（CNNVD-202009-386、CVE-2020-1338）	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-1218 https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-1338
4	Microsoft Excel 安全漏洞（CNNVD-202009-371、CVE-2020-1594）（CNNVD-202009-387、CVE-2020-1335）（CNNVD-202009-372、CVE-2020-1332）（CNNVD-202009-373、CVE-2020-1193）	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-1594 https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-1335 https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-1332 https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-1193
5	Microsoft Dynamics 365 和 Microsoft Dynamics 安全漏洞（CNNVD-202009-490、CVE-2020-16862）（CNNVD-202009-467、CVE-2020-16860）	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-16862 https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-16860
6	Microsoft Windows 安全漏洞（CNNVD-202009-412、CVE-2020-1319）(CNNVD-202009-428、CVE-2020-1129)	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-1319 https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-1129
7	Windows Media 安全漏洞(CNNVD-202009-407、CVE-2020-1508）（CNNVD-202009-399、CVE-2020-1593）	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-1508 https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-1593
8	Microsoft Windows Jet 数据库安全漏洞(CNNVD-202009-434、CVE-2020-1074)（CNNVD-202009-438、CVE-2020-1039）	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-1074 https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-1039
9	Windows GDI 安全漏洞（CNNVD-202009-415、CVE-2020-1285）	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-1285
10	Microsoft 浏览器安全漏洞(CNNVD-202009-368、CVE-2020-0878)	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-0878
11	Microsoft COM 安全漏洞(CNNVD-202009-452、CVE-2020-0922)	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-0922

信息安全漏洞周报

2020 年 9月 3 周

CNNVD **2020 年 9 月 20 日**

根据国家信息安全漏洞库（CNNVD）统计，本周（2020 年 09 月 14 日至 2020 年 09 月 20 日）安全漏洞情况如下：

公开漏洞情况

本周 CNNVD 采集安全漏洞 390 个，与上周（410 个）相比减少了 4.88%。

接报漏洞情况

本周 CNNVD 接报漏洞 634 个，其中信息技术产品漏洞（通用型漏洞）24 个，网络信息系统漏洞（事件型漏洞）610 个。

重大漏洞预警

Microsoft NetLogon 权限提升漏洞（CNNVD-202008-548、CVE-2020-1472）：成功利用漏洞的攻击者可以在未经身份验证的情况下获取域控制器的管理员权限，最终控制目标服务器。Microsoft Windows Server 2008 R2 SP1，Windows Server 2012，Windows Server 2012 R2,Windows Server 2016,Windows Server 2019,Windows Server 1903 版本，Windows Server 1909 版本，Windows Server 2004 版本均受此漏洞影响。

一、公开漏洞情况

根据国家信息安全漏洞库（CNNVD）统计，本周新增安全漏洞 390 个，漏洞新增数量有所下降。从厂商分布来看 Google 公司新增漏洞最多，有 112 个；从漏洞类型来看，跨站脚本类的安全漏洞占比最大，达到 11.79%。新增漏洞中，超危漏洞 16 个，高危漏洞 66 个，中危漏洞 302 个，低危漏洞 6 个。相应修复率分别为 75.00%、89.39%、93.05%和 100.00%。根据补丁信息统计，合计 358 个漏洞已有修复补丁发布，整体修复率为 91.79%。

（一） 安全漏洞增长数量情况

本周 CNNVD 采集安全漏洞 390 与上周（410 个）相比减少了 4.88%。

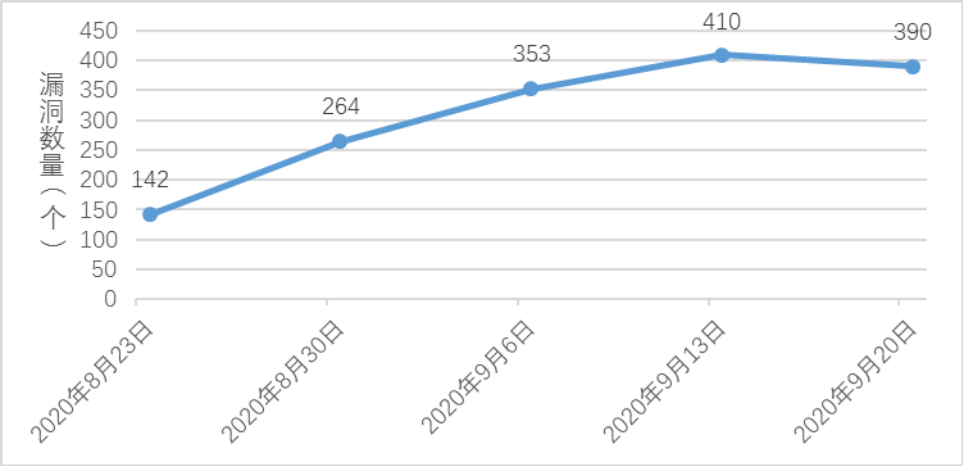

图 1 近五周漏洞新增数量统计图

（二） 安全漏洞分布情况

从厂商分布来看，Google 公司新增漏洞最多，有 112 个。各厂商漏洞数量分布如表 1 所示。

表 1 新增安全漏洞排名前五厂商统计表

序号	厂商名称	漏洞数量（个）	所占比例

1	Google	112	28.72%
2	CloudBees	27	6.92%
3	IBM	16	4.10%
4	Apple	13	3.33%
5	VMware	8	2.05%

本周国内厂商漏洞 4 个，D-Link 公司漏洞数量最多，有 2 个。国内厂商漏洞整体修复率为 100.00%。请受影响用户关注厂商修复情况，及时下载补丁修复漏洞。

从漏洞类型来看，跨站脚本类的安全漏洞占比最大，达到 11.79%。漏洞类型统计如表 2 所示。

表 2 漏洞类型统计表

序号	漏洞类型	漏洞数量（个）	所占比例
1	跨站脚本	46	11.79%
2	缓冲区错误	16	4.10%
3	代码问题	15	3.85%
4	跨站请求伪造	14	3.59%
5	信息泄露	14	3.59%
6	路径遍历	10	2.56%
7	注入	9	2.31%
8	授权问题	7	1.79%
9	默认配置问题	7	1.79%
10	SQL 注入	6	1.54%
11	信任管理问题	4	1.03%
12	输入验证错误	2	0.51%
13	资源管理错误	2	0.51%
14	操作系统命令注入	2	0.51%
15	权限许可和访问控制问题	2	0.51%
16	访问控制错误	1	0.26%
17	配置错误	1	0.26%
18	命令注入	1	0.26%
19	加密问题	1	0.26%
20	安全特征问题	1	0.26%
21	其他	220	56.41%

（三） 安全漏洞危害等级与修复情况

本周共发布超危漏洞 16 个，高危漏洞 66 个，中危漏洞 302 个，低危漏洞 6 个。相应修复率分别为 75.00%、89.39%、93.05%和 100.00%。根据补丁信息统计，合计 358 个漏洞已有修复补丁发布，整体修复率为 91.79%。详细情况如表 3 所示。

表 3 漏洞危害等级与修复情况

序号	危害等级	漏洞数量（个）	修复数量（个）	修复率
1	超危	16	12	75.00%
2	高危	66	59	89.39%
3	中危	302	281	93.05%
4	低危	6	6	100.00%
合计		390	358	91.79%

（四） 本周重要漏洞实例

本期重要漏洞实例如表 4 所示。

表 4 本期重要漏洞实例

序号	漏洞类型	漏洞编号	厂商	漏洞实例	是否修复	危害等级
1	其他	CNNVD-202009-914	Gallagher Group	Gallagher Group Command Centre 安全漏洞	是	超危
2	缓冲区溢出	CNNVD-202009-937	Linux	Linux kernel 缓冲区溢出漏洞	是	高危
3	资源管理错误	CNNVD-202009-1030	Apple	Apple MacOSX Safari 安全漏洞	是	高危

1. Gallagher Group Command Centre 安全漏洞（CNNVD-202009-914）

Gallagher Group Command Centre 是新西兰 Gallagher Group 公司的一款用于 Gallagher 门禁系统的集中控制工具。

Gallagher Group Command Centre 存在安全漏洞，攻击者可利用该漏洞访问所有数据，以下是受影响的产品及版本：8.10 之前的版本 8.10.1134 (MR4)，8.00 之前的版本 8.00.1161 (MR5)，7.90 之前的版本 7.90.991 (MR5)，7.80 之前的版本 7.80.960 (MR2)，7.70 和更早的版本。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://security.gallagher.com/Security-Advisories/CVE-2020-16096

2. Linux kernel 缓冲区溢出漏洞（CNNVD-202009-937）

Linux kernel 是美国 Linux 基金会发布的开源操作系统 Linux 所使用的内核。

Linux 内核 fbcon_redraw_softback()存在缓冲区溢出漏洞，该漏洞允许攻击者触发拒绝服务，并运行代码。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=50145474f6ef4a9c19205b173da6264a644c7489

3. Apple MacOSX Safari 安全漏洞（CNNVD-202009-1030）

Apple Safari 是美国苹果（Apple）公司的一款 Web 浏览器，是 Mac OS X 和 iOS 操作系统附带的默认浏览器。

MacOSX Safari 13.0.2 版本中存在安全漏洞，攻击者可利用该漏洞远程执行代码。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://support.apple.com/en-us/HT211845

二、接报漏洞情况

本周 CNNVD 接报漏洞 634 个，其中信息技术产品漏洞（通用型漏洞）24 个，网络信息系统漏洞（事件型漏洞）610 个。

表 5 本周漏洞报送情况

序号	报送单位	漏洞总量
1	网神信息技术（北京）股份有限公司	307
2	上海斗象信息科技有限公司	168
3	西安四叶草信息技术有限公司	53
4	北京华云安信息技术有限公司	28
5	杭州默安科技有限公司	26
6	星云博创	19
7	山东华鲁科技发展股份有限公司	11
8	北京数字观星科技有限公司	10
9	北京顶象技术有限公司 洞见安全实验室	4
10	美团安全	3
11	北京奇虎科技有限公司	1
12	北京智游网安科技有限公司	1
13	蚂蚁集团	1
14	汉武安全实验室	1
15	苏州极光无限信息技术有限公司	1
报送总计		634

三、接报漏洞预警情况

本周 CNNVD 接报漏洞预警 75 个。

1	报送单位	漏洞总量
1	北京顶象技术有限公司 洞见安全实验室	17
2	杭州迪普科技有限公司	16
3	内蒙古洞明科技有限公司	9
4	恒安嘉新（北京）科技股份公司	7
5	北京华顺信安科技有限公司	5
6	网神信息技术（北京）股份有限公司	3
7	北京神州绿盟科技有限公司	3
8	深信服科技股份有限公司	3
9	北京奇虎科技有限公司	3
10	杭州安恒信息技术股份有限公司	2
11	北京山石网科信息技术有限公司	2
12	内蒙古奥创科技有限公司	2
13	北京知道创宇信息技术股份有限公司	1
14	北京天融信网络安全技术有限公司	1
15	新华三技术有限公司	1
报送总计		75

四、重大漏洞预警

Microsoft NetLogon 权限提升漏洞预警

近日，国家信息安全漏洞库（CNNVD）收到关于 Microsoft

NetLogon 权限提升漏洞（CNNVD-202008-548、CVE-2020-1472）情况的报送。成功利用漏洞的攻击者可以在未经身份验证的情况下获取域控制器的管理员权限，最终控制目标服务器。Microsoft Windows Server 2008 R2 SP1，Windows Server 2012，Windows Server 2012 R2，Windows Server 2016，Windows Server 2019，Windows Server 1903 版本，Windows Server 1909 版本，Windows Server 2004 版本均受此漏洞影响。目前，微软官方已经发布了补丁修复了漏洞，建议用户及时确认是否受到漏洞影响，尽快采取修补措施。

.漏洞介绍

Netlogon 是一个用于为域控制器注册所有 SRV 资源记录的服务。Microsoft Windows NetLogon 中存在提权漏洞，该漏洞是 Windows Server 在实现登录验证的 AES-CFB8 加密算法初始化 IV 时不恰当的使用随机数导致。攻击者可借助事先设计好的应用程序利用该漏洞获取管理员访问权限。

.危害影响

成功利用漏洞的攻击者可以在未经身份验证的情况下获取域控制器的管理员权限，最终控制目标服务器。Microsoft Windows Server 2008 R2 SP1，Windows Server 2012，Windows Server 2012 R2，Windows Server 2016，Windows Server 2019，Windows Server 1903 版本，Windows Server 1909 版本，Windows Server 2004 版本均受此漏洞影响。

.修复建议

目前，微软官方已经发布了补丁修复了漏洞，建议用户及时确认是否受到漏洞影响，尽快采取修补措施。安全更新公告如下：

https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-1472

信息安全漏洞周报

2020 年　9月　　4 周

CNNVD　　**2020 年 9 月 27 日**

根据国家信息安全漏洞库（CNNVD）统计，本周（2020 年 09 月 21 日至 2020 年 09 月 27 日）安全漏洞情况如下：

公开漏洞情况

本周 CNNVD 采集安全漏洞 310 个，与上周（390 个）相比减少了 20.51%。

接报漏洞情况

本周 CNNVD 接报漏洞 1456 个，其中信息技术产品漏洞（通用型漏洞）43 个，网络信息系统漏洞（事件型漏洞）1413 个。

一、公开漏洞情况

根据国家信息安全漏洞库（CNNVD）统计，本周新增安全漏洞 310 个，漏洞新增数量有所下降。从厂商分布来看 Cisco 公司新增漏洞最多，有 52 个；从漏洞类型来看，输入验证错误类的安全漏洞占比最大，达到 13.55%。新增漏洞中，超危漏洞 19 个，高危漏洞 87 个，中危漏洞 198 个，低危漏洞 6 个。相应修复率分别为 100.00%、97.70%、90.91%和 83.33%。根据补丁信息统计，合计 289 个漏洞已有修复补丁发布，整体修复率为 93.23%。

（一） 安全漏洞增长数量情况

本周 CNNVD 采集安全漏洞 310 与上周（390 个）相比减少了 20.51%。

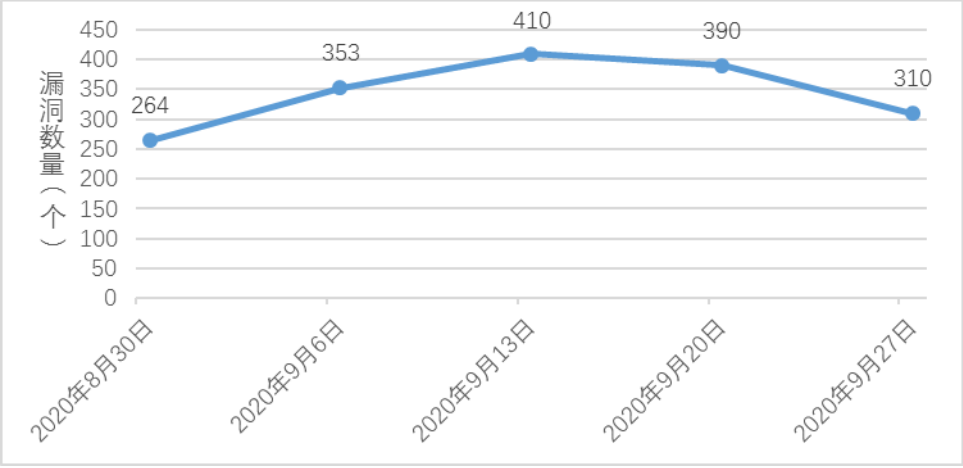

图 1 近五周漏洞新增数量统计图

（二） 安全漏洞分布情况

从厂商分布来看，Cisco 公司新增漏洞最多，有 52 个。各厂商漏洞数量分布如表 1 所示。

表 1 新增安全漏洞排名前五厂商统计表

序号	厂商名称	漏洞数量（个）	所占比例
1	Cisco	52	16.77%
2	Google	33	10.65%
3	IBM	18	5.81%
4	cPanel	18	5.81%
5	CloudBees	7	2.26%

本周国内厂商漏洞 3 个，Lenovo 公司漏洞数量最多，有 2 个。国内厂商漏洞整体修复率为 100.00%。请受影响用户关注厂商修复情况，及时下载补丁修复漏洞。

从漏洞类型来看，输入验证错误类的安全漏洞占比最大，达到 13.55%。漏洞类型统计如表 2 所示。

表 2 漏洞类型统计表

序号	漏洞类型	漏洞数量（个）	所占比例
1	输入验证错误	42	13.55%
2	跨站脚本	26	8.39%
3	代码问题	25	8.06%
4	SQL 注入	20	6.45%
5	缓冲区错误	12	3.87%
6	跨站请求伪造	10	3.23%
7	访问控制错误	5	1.61%
8	路径遍历	5	1.61%
9	资源管理错误	4	1.29%
10	代码注入	4	1.29%
11	信息泄露	3	0.97%
12	加密问题	3	0.97%
13	授权问题	2	0.65%
14	操作系统命令注入	2	0.65%
15	命令注入	1	0.32%
16	权限许可和访问控制问题	1	0.32%

17	信任管理问题	1	0.32%
18	注入	1	0.32%
19	安全特征问题	1	0.32%
20	参数注入	1	0.32%
21	其他	140	45.16%

（三） 安全漏洞危害等级与修复情况

本周共发布超危漏洞 19 个，高危漏洞 87 个，中危漏洞 198 个，低危漏洞 6 个。相应修复率分别为 100.00%、97.70%、90.91%和 83.33%。根据补丁信息统计，合计 289 个漏洞已有修复补丁发布，整体修复率为 93.23%。详细情况如表 3 所示。

表 3 漏洞危害等级与修复情况

序号	危害等级	漏洞数量（个）	修复数量（个）	修复率
1	超危	19	19	100.00%
2	高危	87	85	97.70%
3	中危	198	180	90.91%
4	低危	6	5	83.33%
合计		310	289	93.23%

（四） 本周重要漏洞实例

本期重要漏洞实例如表 4 所示。

表 4 本期重要漏洞实例

序号	漏洞类型	漏洞编号	厂商	漏洞实例	是否修复	危害等级
1	其他	CNNVD-202009-1279	Google	Google Chrome 安全漏洞	是	超危
2	其他	CNNVD-202009-1300	Mozilla 基金会	Mozilla Firefox 安全漏洞	是	高危
3	其他	CNNVD-202009-1392	Cisco	Cisco IOS 和 IOS XE 安全漏洞	是	高危

1. Google Chrome 安全漏洞（CNNVD-202009-1279）

Google Chrome 是美国谷歌（Google）公司的一款 Web 浏览器。

Google Chrome 中扩展程序 85.0.4183.121 之前的版本存在安全漏洞，该漏洞源于策略验证不足，该漏洞允许攻击者通过诱使用户诱安装恶意扩展程序执行沙盒逃脱。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://chromereleases.googleblog.com/2020/09/stable-channel-update-for-desktop_21.html

2. Mozilla Firefox 安全漏洞（CNNVD-202009-1300）

Mozilla Firefox 是美国 Mozilla 基金会的一款开源 Web 浏览器。

Mozilla Firefox 存在安全漏洞。目前尚无此漏洞的相关信息，请随时关注 CNNVD 或厂商公告。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://www.mozilla.org/en-US/firefox/81.0/releasenotes/

3. Cisco IOS 和 IOS XE 安全漏洞（CNNVD-202009-1392）

Cisco IOS 和 IOS XE 都是美国思科（Cisco）公司的一套为其网络设备开发的操作系统。

Cisco IOS XE Web UI 存在安全漏洞，该漏洞源于 Web UI 访问请求的授权不足所致，攻击者可利用该漏洞通过向 Web UI 发送精心设计的 HTTP 请求。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://tools.cisco.com/security/center/content/CiscoSe

curityAdvisory/cisco-sa-webui-auth-bypass-6j2BYUc7

二、接报漏洞情况

本周 CNNVD 接报漏洞 1456 个，其中信息技术产品漏洞（通用型漏洞）43 个，网络信息系统漏洞（事件型漏洞）1413 个。

表 5 本周漏洞报送情况

序号	报送单位	漏洞总量
1	上海斗象信息科技有限公司	589
2	中新网络信息安全股份有限公司	293
3	网神信息技术（北京）股份有限公司	244
4	北京奇虎科技有限公司	114
5	长春嘉诚信息技术股份有限公司	85
6	山东华鲁科技发展股份有限公司	31
7	杭州默安科技有限公司	26
8	安徽长泰信息安全服务有限公司	18
9	杭州海康威视数字技术股份有限公司	14
10	广东东福信息技术有限公司	12
11	中兴通讯	6
12	北京山石网科信息技术有限公司	6
13	重庆梦之想科技有限公司	6
14	北京数字观星科技有限公司	5
15	北京天融信网络安全技术有限公司	2
16	中国电信股份有限公司网络安全产品运营中心	2
17	中国人民银行数字货币研究所	1

18	北京智游网安科技有限公司	1
19	美团安全	1
报送总计		1456

三、接报漏洞预警情况

本周 CNNVD 接报漏洞预警 72 个。

1	报送单位	预警总量
1	北京顶象技术有限公司 洞见安全实验室	16
2	北京华云安信息技术有限公司	15
3	杭州迪普科技有限公司	15
4	深信服科技股份有限公司	7
5	北京启明星辰信息安全技术有限公司	5
6	北京神州绿盟科技有限公司	3
7	北京华顺信安科技有限公司	3
8	北京知道创宇信息技术股份有限公司	2
9	北京奇虎科技有限公司	2
10	杭州安恒信息技术股份有限公司	1
11	北京天融信网络安全技术有限公司	1
12	网神信息技术（北京）股份有限公司	1
13	内蒙古奥创科技有限公司	1
报送总计		72