信息安全漏洞周报

（2020 年第 36 期 总第 540 期）

信息安全测评中心　　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%。

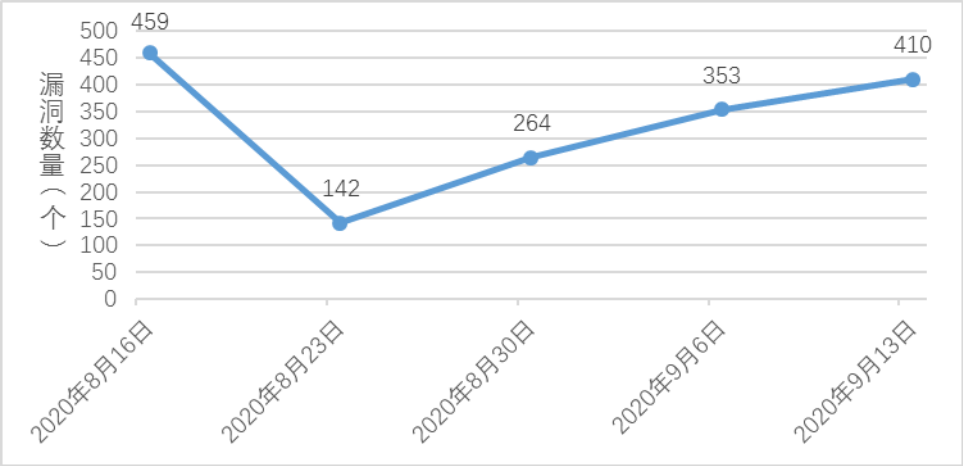

图 1 近五周漏洞新增数量统计图

（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