信息安全漏洞周报

（2020 年第 37 期 总第 541 期）

信息安全测评中心　　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%。

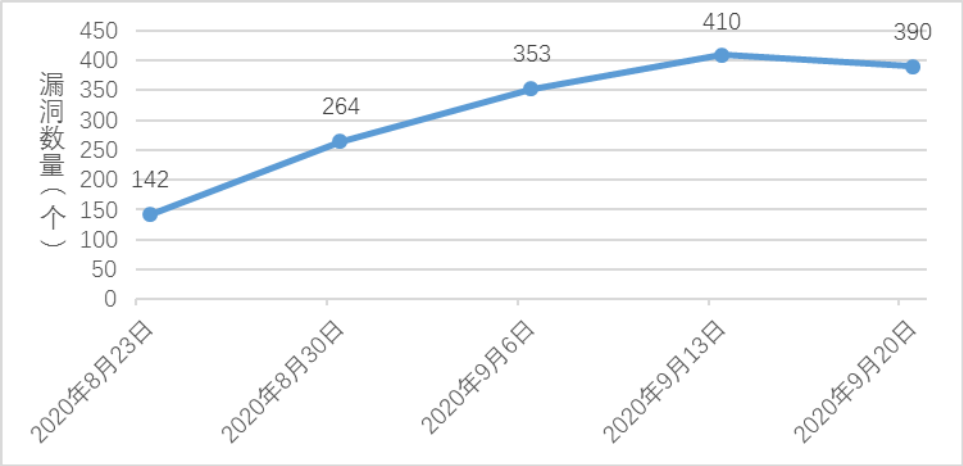

图 1 近五周漏洞新增数量统计图

（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