北京师范大学网络信息安全通告

2020 年 5 月报告

北京师范大学信息网络中心

2020年 6 月

信息安全漏洞周报

（2020 年5 月　　第 1 周 ）

CNNVD　　**2020 年 5 月 10 日**

根据国家信息安全漏洞库（CNNVD）统计，本周（2020 年 05 月 04 日至 2020 年 05 月 10 日）安全漏洞情况如下：

公开漏洞情况

本周 CNNVD 采集安全漏洞 357 个，与上周（284 个）相比增加了 25.70%。

接报漏洞情况

本周 CNNVD 接报漏洞 2101 个，其中信息技术产品漏洞（通用型漏洞）19 个，网络信息系统漏洞（事件型漏洞）2082 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 357 个，漏洞新增数量有所上升。从厂商分布来看 Cisco 公司新增漏洞最多，有 35 个；从漏洞类型来看，缓冲区错误类的安全漏洞占比最大，达到 9.24%。新增漏洞中，超危漏洞 29 个，高危漏洞 138 个，中危漏洞 164 个，低危漏洞 26 个。相应修复率分别为 72.41%、86.23%、79.88%和 80.77%。根据补丁信息统计，合计 292 个漏洞已有修复补丁发布，整体修复率为 81.79%。

（一） 安全漏洞增长数量情况

本周 CNNVD 采集安全漏洞 357 与上周（284 个）相比增多了 25.70%。图 1 为近五周漏洞新增数量统计图。

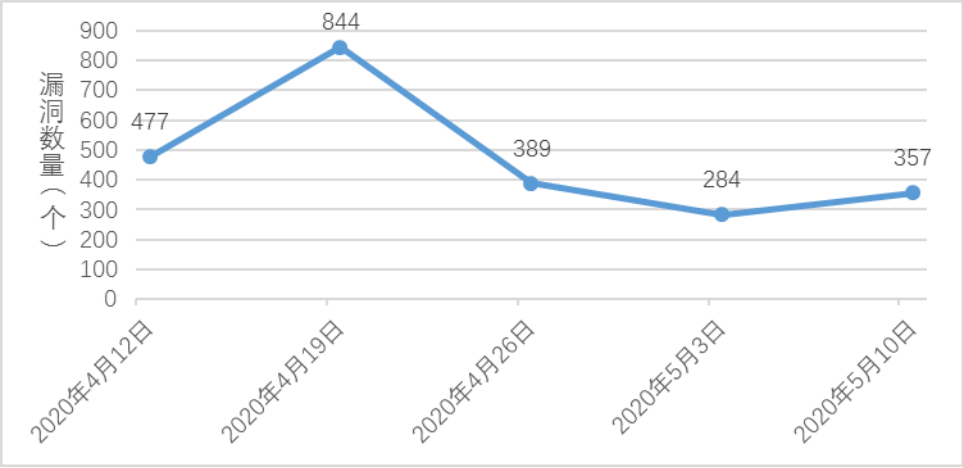

图 1 近五周漏洞新增数量统计图

（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 35 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	35	9.80%
2	Google	26	7.28%
3	Qualcomm	22	6.16%
4	Linux 基金会	14	3.92%
5	Mozilla 基金会	13	3.64%

本周国内厂商漏洞 24 个，Advantech 公司漏洞数量最多，有 8 个。国内厂商漏洞整体修复率为 58.33%。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，缓冲区错误类的安全漏洞占比最大，达到 9.24%。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	缓冲区错误	33	9.24%
2	跨站脚本	28	7.84%
3	输入验证错误	25	7.00%
4	资源管理错误	20	5.60%
5	路径遍历	16	4.48%
6	信息泄露	12	3.36%
7	跨站请求伪造	10	2.80%
8	代码问题	9	2.52%
9	授权问题	7	1.96%
10	SQL 注入	6	1.68%
11	访问控制错误	6	1.68%
12	操作系统命令注入	5	1.40%
13	注入	5	1.40%
14	信任管理问题	5	1.40%
15	竞争条件问题	4	1.12%
16	命令注入	2	0.56%
17	代码注入	2	0.56%
18	数据伪造问题	1	0.28%
19	加密问题	1	0.28%
20	环境问题	1	0.28%
21	数字错误	1	0.28%

22	参数注入	1	0.28%
23	其他	157	43.98%

（三） 安全漏洞危害等级与修复情况

本周共发布超危漏洞 29 个，高危漏洞 138 个，中危漏洞 164 个，低危漏洞 26 个。相应修复率分别为 72.41%、86.23%、79.88%和 80.77%。根据补丁信息统计，合计 292 个漏洞已有修复补丁发布，整体修复率为 81.79%。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	29	21	72.41%
2	高危	138	119	86.23%
3	中危	164	131	79.88%
4	低危	26	21	80.77%
合计		357	292	81.79%

（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	信任管理问题	CNNVD-202005-189	Cisco	Cisco Firepower Management Center 信任管理问题漏洞	是	超危
2	代码注入	CNNVD-202005-030	Apache 基金会	Apache Syncope 代码注入漏洞	是	超危
3	其他	CNNVD-202005-150	Mozilla 基金会	Mozilla Thunderbird、Firefox ESR 和 Firefox 安全漏洞	是	高危

1. Cisco Firepower Management Center 信任管理问题漏洞（CNNVD-202005-189）

Cisco Firepower Management Center（FMC）是美国思科（Cisco）公司的新一代防火墙管理中心软件。

Cisco FMC Software 中存在信任管理问题漏洞，该漏洞源于系统账户使用了默认的静态密码并且系统管理员无法进行更改。远程攻击者可借助此账户利用该漏洞访问系统的敏感部分。

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/CiscoSecurityAdvisory/cisco-sa-fmcua-statcred-weeCcZct

2. Apache Syncope 代码注入漏洞（CNNVD-202005-030）

Apache Syncope 是美国阿帕奇（Apache）基金会的一套用于企业环境中的开源数字身份管理系统。该系统支持身份管理、角色配置等。

Apache Syncope 2.1.6 之前版本中存在安全漏洞。攻击者可利用该漏洞注入任意的 Java EL 表达式，执行任意的 Java 代码。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

http://syncope.apache.org/security

3. Mozilla Thunderbird、Firefox ESR 和 Firefox 安全漏洞（CNNVD-202005-150）

Mozilla Firefox 等都是美国 Mozilla 基金会的产品。Mozilla Firefox 是一款开源 Web 浏览器。Mozilla Firefox ESR 是 Firefox(Web 浏览器)的一个延长支持版本。Mozilla Thunderbird 是一套从 Mozilla Application Suite 独立出来的电子邮件客户端软件。

Mozilla Thunderbird 68.8.0 之前版本、Firefox ESR 68.8 之前版本和 Firefox 76 之前版本中存在安全漏洞。攻击者可借助特制的网站利用该漏洞在受影响系统上执行任意代码或造成拒绝服务。

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/security/advisories/mfsa2020-16/

https://www.mozilla.org/en-US/security/advisories/mfsa2020-17/

https://www.mozilla.org/en-US/security/advisories/mfsa2020-18/

二、接报漏洞情况

本周 CNNVD 接报漏洞 2101 个，其中信息技术产品漏洞（通用型漏洞）19 个，网络信息系统漏洞（事件型漏洞）2082 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	1162
2	上海斗象信息科技有限公司司	697
3	长春嘉诚信息技术股份有限公司	151
4	山东新潮信息技术有限公司	25
5	内蒙古奥创科技有限公司	24
6	广州锦行网络科技有限公司	20
7	中兴通讯	8

8	杭州安恒信息技术股份有限公司	3
9	上海安识网络科技有限公司	3
10	浙江宇视科技有限公司	2
11	北京长亭科技有限公司	2
12	北京智游网安科技有限公司	2
13	绿盟科技集团股份有限公司工业物联网安全实验室	1
14	北京恒济引航科技股份有限公司	1
报送总计		2101

信息安全漏洞周报

（2020 年5 月　　第 2 周 ）

CNNVD　　2020 年 5 月 17 日

根据国家信息安全漏洞库（CNNVD）统计，本周（2020 年 05 月 11 日至 2020 年 05 月 17 日）安全漏洞情况如下：

公开漏洞情况

本周 CNNVD 采集安全漏洞 414 个，与上周（357 个）相比增加了 15.97%。

接报漏洞情况

本周 CNNVD 接报漏洞 8687 个，其中信息技术产品漏洞（通用型漏洞）34 个，网络信息系统漏洞（事件型漏洞）8653 个。

重大漏洞预警

微软多个安全漏洞：近包括 Microsoft SharePoint 安全漏洞（CNNVD-202005-567、CVE-2020-1024）、Microsoft Excel 安全漏洞（CNNVD-202005-555、CVE-2020-0901）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。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 414 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 111 个；从漏洞类型来看，缓冲区错误类的安全漏洞占比最大，达到 17.63%。新增漏洞中，超危漏洞 47 个，高危漏洞 224 个，中危漏洞 129 个，低危漏洞 14 个。相应修复率分别为 93.62%、92.86%、88.37%和 78.57%。根据补丁信息统计，合计 377 个漏洞已有修复补丁发布，整体修复率为 91.06%。

（一） 安全漏洞增长数量情况

本周 CNNVD 采集安全漏洞 414 与上周（357 个）相比增多了 15.97%。图 1 为近五周漏洞新增数量统计图。

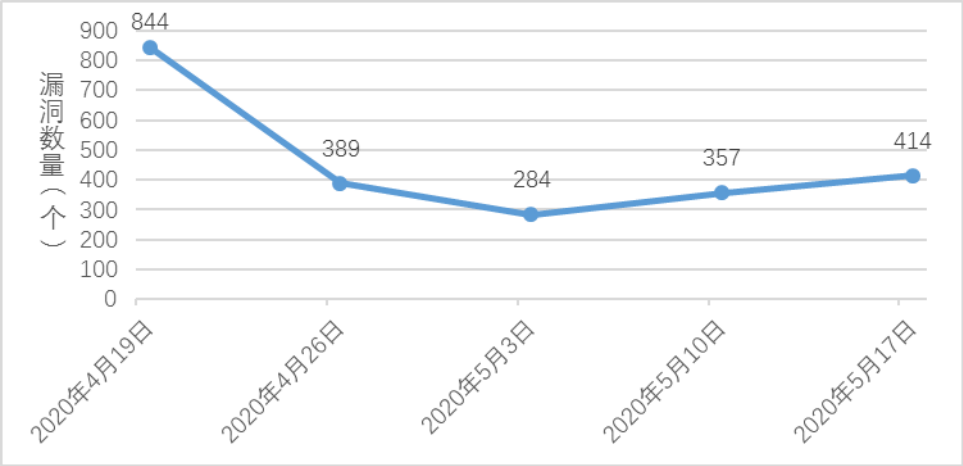

图 1 近五周漏洞新增数量统计图

（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 111 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	111	26.81%
2	Adobe	36	8.70%
3	Palo Alto Networks	24	5.80%
4	IBM	23	5.56%
5	SAP	19	4.59%

本周国内厂商漏洞 6 个，Dahua 公司漏洞数量最多，有 3 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，缓冲区错误类的安全漏洞占比最大，达到 17.63%。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	缓冲区错误	73	17.63%
2	跨站脚本	26	6.28%
3	信息泄露	24	5.80%
4	输入验证错误	21	5.07%
5	代码问题	16	3.86%
6	资源管理错误	9	2.17%
7	注入	8	1.93%
8	路径遍历	7	1.69%
9	访问控制错误	6	1.45%
10	授权问题	5	1.21%
11	SQL 注入	5	1.21%
12	跨站请求伪造	4	0.97%
13	操作系统命令注入	4	0.97%
14	竞争条件问题	4	0.97%
15	数据伪造问题	4	0.97%
16	信任管理问题	3	0.72%
17	代码注入	2	0.48%
18	日志信息泄露	2	0.48%
19	后置链接	1	0.24%
20	其他	190	45.89%

（三） 安全漏洞危害等级与修复情况

本周共发布超危漏洞 47 个，高危漏洞 224 个，中危漏洞 129 个，低危漏洞 14 个。相应修复率分别为 93.62%、92.86%、88.37%和 78.57%。根据补丁信息统计，合计 377 个漏洞已有修复补丁发布，整体修复率为 91.06%。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	47	44	93.62%
2	高危	224	208	92.86%
3	中危	129	114	88.37%
4	低危	14	11	78.57%
合计		414	377	91.06%

（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	访问控制错误	CNNVD-202005-800	Emerson Electric	多款 Emerson Electric 产品访问控制错误漏洞	是	超危
2	代码问题	CNNVD-202005-442	Apache 软件基金会	Apache log4net 代码问题漏洞	是	超危
3	其他	CNNVD-202005-549	Microsoft	Microsoft Internet Explorer 安全漏洞	是	高危

1. 多款 Emerson Electric 产品访问控制错误漏洞（CNNVD-202005-800）

Emerson Electric Wireless 1410 Gateway 等都是美国艾默生

电气（Emerson Electric）公司的一款智能无线网关产品。

Emerson Electric Wireless 1410 Gateway 4.6.43 版本至 4.7.84 版本、Wireless 1420 Gateway 4.6.43 版本至 4.7.84 版本和 Wireless 1552WU Gateway 4.6.43 版本至 4.7.84 版本中的用于配置内部网关防火墙的代码存在访问控制错误漏洞。当网关的 VLAN 功能被启用时，攻击者可利用该漏洞向网关发送命令，进而转发到终端用户的无线设备上。

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://www.emerson.com/

2. Apache Syncope 代码注入漏洞（CNNVD-202005-442）

Apache log4net 是美国阿帕奇（Apache）软件基金会的一款日志输出工具。

Apache log4net 2.0.8 之前版本中 log4net 配置文件的解析过程存在代码问题漏洞。攻击者可借助特制 XML 内容利用该漏洞迫使系统接受任意配置文件。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://issues.apache.org/jira/browse/LOG4NET-575

3. Microsoft Internet Explorer 安全漏洞（CNNVD-202005-549）

Microsoft Internet Explorer（IE）是美国微软（Microsoft）公司的一款 Windows 操作系统附带的 Web 浏览器。

Microsoft Internet Explorer 9 版本和 11 版本中存在远程代码执行漏洞，该漏洞源于程序没有正确地访问内存对象。攻击者可利

用该漏洞在当前用户的上下文中执行任意代码，损坏内存。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-1062

二、接报漏洞情况

本周 CNNVD 接报漏洞 8687 个，其中信息技术产品漏洞（通用型漏洞）34 个，网络信息系统漏洞（事件型漏洞）8653 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	7124
2	上海斗象信息科技有限公司司	1170
3	长春嘉诚信息技术股份有限公司	132
4	北京华云安信息技术有限公司	66
5	北京赋云安运营科技有限公司	50
6	安徽华云网安信息技术有限公司	46
7	山东新潮信息技术有限公司	25
8	远江盛邦(北京)网络安全科技股份有限公司	20
9	杭州默安科技有限公司	17
10	绿盟科技集团股份有限公司工业物联网安全实验室	10
11	深圳开源互联网安全技术有限公司	10
12	中兴通讯	5
13	北京中金安服科技有限公司	4

14	北京圣博润高新技术股份有限公司	3
15	北京启明星辰信息安全技术有限公司	1
16	北京智游网安科技有限公司	1
17	河南听潮盛世信息技术有限公司	1
18	浙江宇视科技有限公司	1
19	南京中新赛克科技有限责任公司	1
报送总计		8687

三、重大漏洞预警

CNNVD 关于微软多个安全漏洞的通报

近日，微软官方发布了多个安全漏洞的公告，包括 Microsoft SharePoint 安全漏洞（CNNVD-202005-567、CVE-2020-1024）、Microsoft Excel 安全漏洞（CNNVD-202005-555、CVE-2020-0901）、Internet Explorer 内存损坏漏洞（CNNVD-202005-549、CVE-2020-1062）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 5 月 13 日，微软发布 2020 年 5 月份安全更新，共 111 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 Microsoft Windows、Internet Explorer、Office、SahrePoint、Win32k 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 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 SharePoint 安全漏洞（CNNVD-202005-567、CVE-2020-1024）（CNNVD-202005-565、CVE-2020-1069）（CNNVD-202005-566、CVE-2020-1023）（CNNVD-202005-561、CVE-2020-1102）

漏洞简介：当软件无法检查应用程序包的源标记时，Microsoft SharePoint 会触发远程代码执行漏洞。成功利用此漏洞的攻击者可以在 SharePoint 应用程序池和 SharePoint 服务器场帐户的上下文中运行任意代码。攻击者必须诱使用户将经过特殊设计的 SharePoint 应用程序包上传到受影响版本的 SharePoint，才能利用此漏洞。

2、Microsoft Windows Graphics Components 安全漏洞（CNNVD-202005-613、CVE-2020-1153）

漏洞简介：Microsoft 图形组件在内存中处理对象的方式中存在远程代码执行漏洞。成功利用该漏洞的攻击者可以对目标系统执行任意代码。若要利用该漏洞，攻击者需要诱使用户打开一个特制的文件。

3、Microsoft Windows 和 Windows Server 安全漏洞（CNNVD-202005-585、CVE-2020-1166）、（CNNVD-202005-583、CVE-2020-1165）

漏洞简介： 当 Windows 不正确地处理对剪贴板服务的调用时，存在特权提升漏洞。成功利用此漏洞的攻击者可以在本地系统的安全上下文中运行任意代码。攻击者可随后安装程序；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。

4、Microsoft Edge PDF Reader 安全漏洞（CNNVD-202005-540、CVE-2020-1096）（CNNVD-202004-694、CVE-2020-0906）

漏洞简介：当 Microsoft Edge PDF 阅读器不正确地处理内存中的对象时，存在远程代码执行漏洞。该漏洞可能以一种使攻击者可以在当前用户的环境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用户权限登录，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；或者创建拥有完全用户权限的新帐户。

5、Microsoft Excel 资源管理错误漏洞（CNNVD-202005-555、CVE-2020-0901）

漏洞简介：当 Microsoft Excel 软件无法正确处理内存中的对象时，会触发远程代码执行漏洞。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用户权限登录，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；或者创建拥有完全用户权限的新帐户。与拥有管理员权限的用户相比，帐户被配置为拥有较少权限的用户受到的影响更小。

6、Microsoft Internet Explorer 安全漏洞（CNNVD-202005-549、CVE-2020-1062）

漏洞简介：当 Internet Explorer 不正确地访问内存中的对象时，会触发远程代码执行漏洞。该漏洞可能以一种攻击者可以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用户权限登录，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；或者创建拥有完全用户权限的新帐户。

7、Microsoft Windows Jet Database Engine 安全漏洞（CNNVD-202005-582、CVE-2020-1174）（CNNVD-202005-581、CVE-2020-1175）（CNNVD-202005-580、CVE-2020-1176）

漏洞简介：当 Windows Jet 数据库引擎不正确地处理内存中的对象时，会触发远程代码执行漏洞。成功利用此漏洞的攻击者可以在受害者系统上执行任意代码。

8、Microsoft Internet Explorer VBScript Engine 安全漏洞（CNNVD-202005-553、CVE-2020-1035）（CNNVD-202005-550、CVE-2020-1060）（CNNVD-202005-545、CVE-2020-1093）（CNNVD-202005-569、CVE-2020-1058）

漏洞简介：VBScript 引擎处理内存中对象的方式中存在远程代码执行漏洞。该漏洞可能以一种攻击者可以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用户权限登录，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；或者创建拥有完全用户权限的新帐户。

. 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 SharePoint 安全漏洞（CNNVD-202005-567、CVE-2020-1024）（CNNVD-202005-565、CVE-2020-1069）（CNNVD-202005-566、CVE-2020-1023）（CNNVD-202005-561、CVE-2020-1102）	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-1024 https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-1069 https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-1023 https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-1102
2	Microsoft Windows Graphics Components 安全漏洞（CNNVD-202005-613、CVE-2020-1153）	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-1153
3	Microsoft Windows 和 Windows Server 安全漏洞（CNNVD-202005-585、CVE-2020-1166）、（CNNVD-202005-583、CVE-2020-1165）	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-1166 https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-1165
4	Microsoft Edge PDF Reader 安全漏洞（CNNVD-202005-540、CVE-2020-1096）（CNNVD-202004-694、CVE-2020-0906）	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-1096

5	Microsoft Excel 资源管理错误漏洞（CNNVD-202005-555、CVE-2020-0901）	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-0901
6	Microsoft Internet Explorer 安全漏洞（CNNVD-202005-549、CVE-2020-1062）	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-1062
7	Microsoft Windows Jet Database Engine 安全漏洞（CNNVD-202005-582、CVE-2020-1174）（CNNVD-202005-581、CVE-2020-1175）（CNNVD-202005-580、CVE-2020-1176）	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-1174 https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-1175 https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-1176
8	Microsoft Internet Explorer VBScript Engine 安全漏洞（CNNVD-202005-553、CVE-2020-1035）（CNNVD-202005-550、CVE-2020-1060）（CNNVD-202005-545、CVE-2020-1093）（CNNVD-202005-569、CVE-2020-1058）	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-0907 https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-0687

信息安全漏洞周报

（2020 年5 月　　第 3 周 ）

CNNVD　　2020 年 5 月 2 4 日

根据国家信息安全漏洞库（CNNVD）统计，本周（2020 年 05 月 18 日至 2020 年 05 月 24 日）安全漏洞情况如下：

公开漏洞情况

本周 CNNVD 采集安全漏洞 231 个，与上周（414 个）相比减少了 44.20%。

接报漏洞情况

本周 CNNVD 接报漏洞 1666 个，其中信息技术产品漏洞（通用型漏洞）82 个，网络信息系统漏洞（事件型漏洞）1584 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 231 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 28 个；从漏洞类型来看，缓冲区错误类的安全漏洞占比最大，达到 10.39%。新增漏洞中，超危漏洞 29 个，高危漏洞 80 个，中危漏洞 114 个，低危漏洞 8 个。相应修复率分别为 62.07%、81.25%、74.56%和 87.50%。根据补丁信息统计，合计 175 个漏洞已有修复补丁发布，整体修复率为 75.76%。

（一） 安全漏洞增长数量情况

本周 CNNVD 采集安全漏洞 231 与上周（414 个）相比减少了 44.20%。

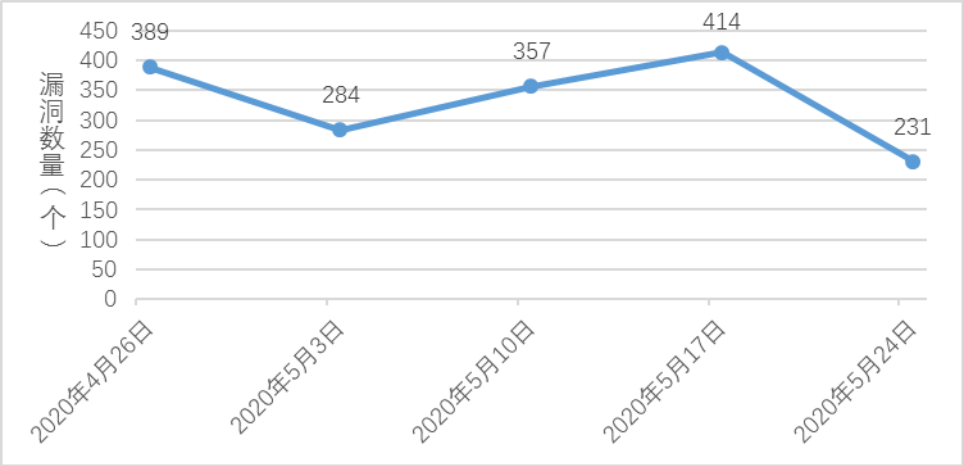

图 1 近五周漏洞新增数量统计图

（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 28 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	28	12.12%
2	Cisco	6	2.60%
3	IBM	5	2.16%
4	rConfig	5	2.16%
5	Microsoft	4	1.73%

本周国内厂商漏洞 5 个，Huawei 公司漏洞数量最多，有 2 个。国内厂商漏洞整体修复率为 40.00%。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，缓冲区错误类的安全漏洞占比最大，达到 10.39%。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	缓冲区错误	24	10.39%
2	输入验证错误	24	10.39%
3	跨站脚本	22	9.52%
4	信息泄露	15	6.49%
5	资源管理错误	15	6.49%
6	代码问题	8	3.46%
7	跨站请求伪造	8	3.46%
8	注入	7	3.03%
9	授权问题	4	1.73%
10	SQL 注入	4	1.73%
11	信任管理问题	3	1.30%
12	环境问题	3	1.30%
13	路径遍历	2	0.87%
14	访问控制错误	2	0.87%
15	参数注入	2	0.87%
16	操作系统命令注入	1	0.43%
17	数据伪造问题	1	0.43%
18	代码注入	1	0.43%
19	后置链接	1	0.43%
20	加密问题	1	0.43%
21	安全特征问题	1	0.43%

22	其他	82	35.50%

（三） 安全漏洞危害等级与修复情况

本周共发布超危漏洞 29 个，高危漏洞 80 个，中危漏洞 114 个，低危漏洞 8 个。相应修复率分别为 62.07%、81.25%、74.56%和 87.50%。根据补丁信息统计，合计 175 个漏洞已有修复补丁发布，整体修复率为 75.76%。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	29	18	62.07%
2	高危	80	65	81.25%
3	中危	114	85	74.56%
4	低危	8	7	87.50%
合计		231	175	75.76%

（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-202005-959	Emerson Electric	Emerson Electric OpenEnterprise 安全漏洞	是	超危
2	代码问题	CNNVD-202005-1078	Apache 软件基金会	Apache Tomcat 代码问题漏洞	是	超危
3	其他	CNNVD-202005-946	Google	Google Chrome 安全漏洞	是	高危

1. Emerson Electric OpenEnterprise 安全漏洞（CNNVD-202005-959）

Emerson Electric OpenEnterprise 是美国艾默生电气（Emerson

Electric）公司的一套主要用于远程石油和天然气应用的数据采集与监控系统（SCADA）。

Emerson Electric OpenEnterprise 3.3.4 及之前版本中存在安全漏洞。攻击者可利用该漏洞以系统权限执行任意命令或执行代码。

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://www.emerson.com/

2. Apache Tomcat 代码问题漏洞（CNNVD-202005-1078）

Apache Tomcat 是美国阿帕奇（Apache）软件基金会的一款轻量级 Web 应用服务器。该程序实现了对 Servlet 和 JavaServer Page（JSP）的支持。

Apache Tomcat 中存在安全漏洞。攻击者可通过控制服务器上文件的内容和名称等方法利用该漏洞执行代码。以下产品及版本受到影响：Apache Tomcat 10.0.0-M1 版本至 10.0.0-M4 版本，9.0.0.0.M1 版本至 9.0.34 版本，8.5.0 版本至 8.5.54 版本，7.0.0 版本至 7.0.103 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://tomcat.apache.org/security.html

3. Google Chrome 安全漏洞（CNNVD-202005-946）

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

Google Chrome 83.0.4103.61 之前版本（OS X）中的安装程序存在安全漏洞。攻击者可借助特制的文件利用该漏洞提升权限。

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/2020/05/stable-channel-update-for-desktop_19.html

二、接报漏洞情况

本周 CNNVD 接报漏洞 1666 个，其中信息技术产品漏洞（通用型漏洞）82 个，网络信息系统漏洞（事件型漏洞）1584 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	1105
2	网神信息技术（北京）股份有限公司	275
3	长春嘉诚信息技术股份有限公司	142
4	深圳开源互联网安全技术有限公司	63
5	太极计算机股份有限公司	37
6	内蒙古奥创科技有限公司	18
7	北京奇虎科技有限公司	10
8	中国信息安全测评中心华中测评中心（湖南省信息安全测评中心）	6
9	北京圣博润高新技术股份有限公司	5
10	北京数字观星科技有限公司	2
11	广西壮族自治区信息安全测评中心	1
12	郑州大学	1
13	个人	1
报送总计		1666

信息安全漏洞周报

（2020 年5 月　　第 4 周 ）

CNNVD　　2020 年 5 月 31 日

根据国家信息安全漏洞库（CNNVD）统计，本周（2020 年 05 月 25 日至 2020 年 05 月 31 日）安全漏洞情况如下：

公开漏洞情况

本周 CNNVD 采集安全漏洞 184 个，与上周（231 个）相比减少了 20.35%。

接报漏洞情况

本周 CNNVD 接报漏洞 3923 个，其中信息技术产品漏洞（通用型漏洞）40 个，网络信息系统漏洞（事件型漏洞）3883 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 184 个，漏洞新增数量有所下降。从厂商分布来看 Apple 公司新增漏洞最多，有 62 个；从漏洞类型来看，缓冲区错误类的安全漏洞占比最大，达到 10.33%。新增漏洞中，超危漏洞 14 个，高危漏洞 87 个，中危漏洞 66 个，低危漏洞 17 个。相应修复率分别为 85.71%、95.40%、96.97%和 100.00%。根据补丁信息统计，合计 176 个漏洞已有修复补丁发布，整体修复率为 95.65%。

（一） 安全漏洞增长数量情况

本周 CNNVD 采集安全漏洞 184 与上周（231 个）相比减少了 20.35%。

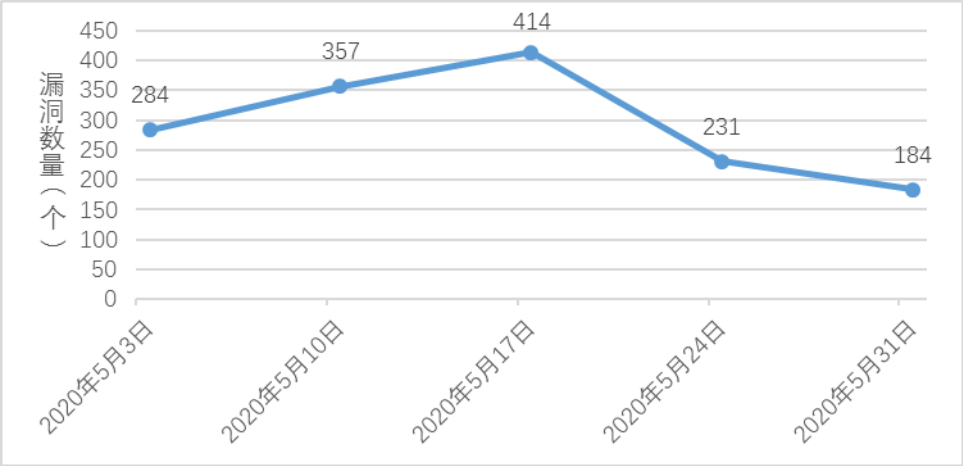

图 1 近五周漏洞新增数量统计图

（二） 安全漏洞分布情况

从厂商分布来看，Apple 公司新增漏洞最多，有 62 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	Apple	62	33.70%
2	IBM	20	10.87%
3	Huawei	7	3.80%
4	Centreon	4	2.17%
5	Trend Micro	4	2.17%

本周国内厂商漏洞 12 个，Huawei 公司漏洞数量最多，有 7 个。国内厂商漏洞整体修复率为 91.67%。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，缓冲区错误类的安全漏洞占比最大，达到 10.33%。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	缓冲区错误	19	10.33%
2	跨站脚本	17	9.24%
3	信息泄露	13	7.07%
4	输入验证错误	9	4.89%
5	代码问题	9	4.89%
6	信任管理问题	6	3.26%
7	跨站请求伪造	5	2.72%
8	授权问题	5	2.72%
9	访问控制错误	4	2.17%
10	资源管理错误	3	1.63%
11	路径遍历	3	1.63%
12	操作系统命令注入	3	1.63%
13	加密问题	3	1.63%
14	代码注入	1	0.54%
15	竞争条件问题	1	0.54%
16	其他	83	45.11%

（三） 安全漏洞危害等级与修复情况

本周共发布超危漏洞 14 个，高危漏洞 87 个，中危漏洞 66 个，低危漏洞 17 个。相应修复率分别为 85.71%、95.40%、96.97%和 100.00%。根据补丁信息统计，合计 176 个漏洞已有修复补丁发布，整体修复率为 95.65%。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	14	12	85.71%
2	高危	87	83	95.40%
3	中危	66	64	96.97%
4	低危	17	17	100.00%
合计		184	176	95.65%

（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-202005-1444	Micro Focus	Micro Focus Service Management Automation 安全漏洞	是	超危
2	其他	CNNVD-202005-1397	bbPress	WordPress bbPress 安全漏洞	是	超危
3	其他	CNNVD-202005-1258	Apple	多款 Apple 产品 WebKit 组件安全漏洞	是	高危

1. Micro Focus Service Management Automation 安全漏洞（CNNVD-202005-1444）

Micro Focus Service Management Automation（SMA）是英国

Micro Focus 公司的一套信息技术服务管理软件解决方案。

Micro Focus SMA 2018.05 版本至 2020.02 版本中存在安全漏洞。攻击者可利用该漏洞未授权访问 Container Deployment Foundation。

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://www.microfocus.com/

2. WordPress bbPress 安全漏洞（CNNVD-202005-1397）

WordPress 是 WordPress 基金会的一套使用 PHP 语言开发的博客平台。该平台支持在 PHP 和 MySQL 的服务器上架设个人博客网站。bbPress 是使用在其中的一个论坛插件。

WordPress bbPress 2.6.5 之前版本中存在安全漏洞。攻击者可利用该漏洞提升权限。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://bbpress.org/blog/2020/05/bbpress-2-6-5-is-out/

3. 多款 Apple 产品 WebKit 组件安全漏洞（CNNVD-202005-1258）

Apple iOS 等都是美国苹果（Apple）公司的产品。Apple iOS 是一套为移动设备所开发的操作系统。Apple tvOS 是一套智能电视操作系统。Apple iPadOS 是一套用于 iPad 平板电脑的操作系统。WebKit 是其中的一个 Web 浏览器引擎组件。

多款 Apple 产品中的 WebKit 组件存在安全漏洞。攻击者可借助特制 Web 内容利用该漏洞执行任意代码。以下产品及版本受到影响：Apple watchOS 6.2.5 之前版本；tvOS 13.4.5 之前版本；iOS 13.5 之前版本；iPadOS 13.5 之前版本；基于 Windows 平台的 iTunes

12.10.7 之前版本;基于 Windows 平台的 iCloud 7.19 之前版本,11.2 之前版本; Safari 13.1.1 之前版本。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://support.apple.com/zh-cn/HT211168

https://support.apple.com/zh-cn/HT211171

https://support.apple.com/zh-cn/HT211175

https://support.apple.com/zh-cn/HT211177

https://support.apple.com/zh-cn/HT211178

https://support.apple.com/zh-cn/HT211179

https://support.apple.com/zh-cn/HT211181

二、接报漏洞情况

本周 CNNVD 接报漏洞 3923 个，其中信息技术产品漏洞（通用型漏洞）40 个，网络信息系统漏洞（事件型漏洞）3883 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	1855
2	上海斗象信息科技有限公司	1735
3	长春嘉诚信息技术股份有限公司	74
4	西安四叶草信息技术有限公司	59
5	杭州海康威视数字技术股份有限公司	57
6	星云博创科技有限公司	34
7	杭州默安科技有限公司	20

8	北京华云安信息技术有限公司	16
9	北京数字观星科技有限公司	12
10	上海谋乐网络科技有限公司	11
11	浙江宇视科技有限公司	6
12	杭州安恒信息技术股份有限公司	6
13	上海银基信息安全技术股份有限公司	5
14	北京江南天安科技有限公司	4
15	中兴通讯	4
16	绿盟科技集团股份有限公司安全研究部	3
17	安徽华云网安信息技术有限公司	2
18	北京赋云安运营科技有限公司	2
19	北京圣博润高新技术股份有限公司	2
20	北京天融信网络安全技术有限公司	2
21	北京智游网安科技有限公司	2
22	山东泽鹿安全技术有限公司	2
23	个人	2
24	安全邦（北京）信息技术有限公司	1
25	北京威努特技术有限公司	1
26	北京邮电大学	1
27	美国印第安纳大学伯明顿分校，中国科学院信息工程研究所	1
28	上海安识网络科技有限公司	1
29	天津市兴先道科技有限公司	1
30	掌控安全	1

31	郑州大学	1
报送总计		3923