信息安全漏洞周报

（2020 年第 32 期 总第 536 期）

信息安全测评中心　　2020 年 8 月 16 日

根据国家信息安全漏洞库（CNNVD）统计，本周（2020 年 08 月 10 日至 2020 年 08 月 16 日）安全漏洞情况如下：

公开漏洞情况

本周 CNNVD 采集安全漏洞 459 个，与上周（272 个）相比增加了 68.75%。

接报漏洞情况

本周 CNNVD 接报漏洞 2642 个，其中信息技术产品漏洞（通用型漏洞）27 个，网络信息系统漏洞（事件型漏洞）2615 个。

重大漏洞预警

Apache Struts2 S2-059 安全漏洞（CNNVD-202008-743、CVE-2019-0230）：成功利用漏洞的攻击者可能对目标系统执行恶意代码。Apache Struts 2.0.0 - Apache Struts 2.5.20 等版本均受此漏洞影响。目前，Apache 官方已经发布了版本更新修复了该漏洞。建议用户及时确认 Apache Struts 产品版本，如受影响，请及时采取修补措施。

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 459 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 120 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 12.42%。新增漏洞中，超危漏洞 35 个，高危漏洞 221 个，中危漏洞 186 个，低危漏洞 17 个。相应修复率分别为 94.29%、95.02%、84.41%和 88.24%。根据补丁信息统计，合计 415 个漏洞已有修复补丁发布，整体修复率为 90.41%。

（一） 安全漏洞增长数量情况

本周 CNNVD 采集安全漏洞 459 与上周（272 个）相比增多了 68.75%。

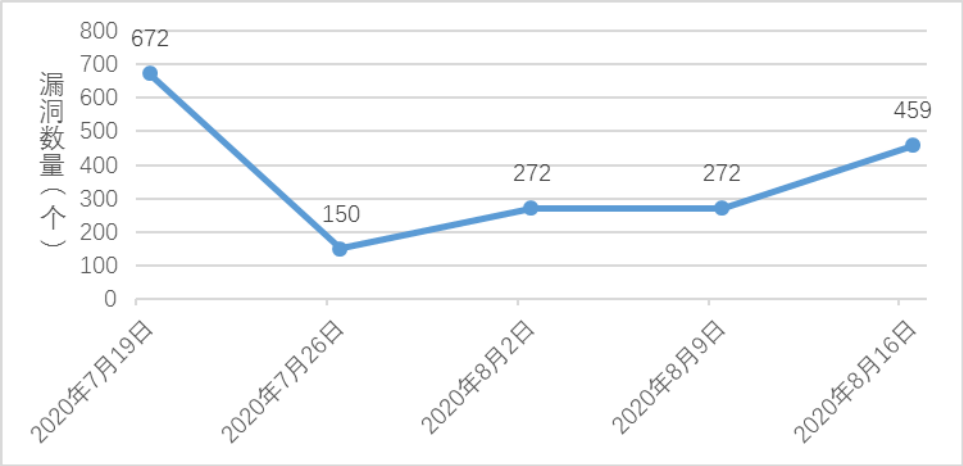

图 1 近五周漏洞新增数量统计图

（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 120 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	120	26.14%
2	Intel	50	10.89%
3	Adobe	31	6.75%
4	Google	18	3.92%
5	GitLab	13	2.83%

本周国内厂商漏洞 11 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 72.73%。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 12.42%。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	57	12.42%
2	跨站脚本	36	7.84%
3	信息泄露	24	5.23%
4	资源管理错误	18	3.92%
5	路径遍历	14	3.05%
6	代码问题	11	2.40%
7	授权问题	10	2.18%
8	输入验证错误	9	1.96%
9	SQL 注入	6	1.31%
10	访问控制错误	4	0.87%
11	跨站请求伪造	4	0.87%
12	代码注入	4	0.87%
13	加密问题	3	0.65%
14	信任管理问题	2	0.44%
15	注入	2	0.44%
16	数字错误	2	0.44%
17	操作系统命令注入	1	0.22%
18	竞争条件问题	1	0.22%
19	数据伪造问题	1	0.22%
20	命令注入	1	0.22%
21	其他	248	54.03%

（三） 安全漏洞危害等级与修复情况

本周共发布超危漏洞 35 个，高危漏洞 221 个，中危漏洞 186 个，低危漏洞 17 个。相应修复率分别为 94.29%、95.02%、84.41%和 88.24%。根据补丁信息统计，合计 415 个漏洞已有修复补丁发布，整体修复率为 90.41%。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	35	33	94.29%
2	高危	221	210	95.02%
3	中危	186	157	84.41%
4	低危	17	15	88.24%
合计		459	415	90.41%

（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-202008-548	Microsoft	Microsoft Windows NetLogon 安全漏洞	是	超危
2	注入	CNNVD-202008-673	IBM	IBM WebSphere Application Server 注入漏洞	是	超危
3	其他	CNNVD-202008-743	Apache 软件基金会	Apache Struts 安全漏洞	是	高危

1. Microsoft Windows NetLogon 安全漏洞（CNNVD-202008-548）

Microsoft Windows 和 Microsoft Windows Server 都是美国微软（Microsoft）公司的产品。Microsoft Windows 是一套个人设备使用的操作系统。Microsoft Windows Server 是一套服务器操作系

统。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。攻击者可借助特制应用程序利用该漏洞获取管理员访问权限。以下产品及版本受到影响：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。

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-2020-1472

2. IBM WebSphere Application Server 注入漏洞（CNNVD-202008-673）

IBM WebSphere Application Server（WAS）是美国 IBM 公司的一款应用服务器产品。该产品是 JavaEE 和 Web 服务应用程序的平台，也是 IBMWebSphere 软件平台的基础。

IBM WAS 7.0 版本、8.0 版本、8.5 版本和 9.0 版本中存在注入漏洞。远程攻击者可利用该漏洞执行任意代码。

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/security-bulletin-websphere-application-server-vulnerable-remote-code-execution-vulnerability-cve-2020-4589

3. Apache Struts 安全漏洞（CNNVD-202008-743）

Apache Struts 是美国阿帕奇（Apache）软件基金会的一个开源项目，是一套用于创建企业级 Java Web 应用的开源 MVC 框架，主要提供两个版本框架产品，Struts 1 和 Struts 2。

Apache Struts 2.0.0 版本至 2.5.20 版本中存在安全漏洞。攻击者可借助特制的请求利用该漏洞执行代码。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://cwiki.apache.org/confluence/display/ww/s2-059

二、接报漏洞情况

本周 CNNVD 接报漏洞 2642 个，其中信息技术产品漏洞（通用型漏洞）27 个，网络信息系统漏洞（事件型漏洞）2615 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	1890
2	上海斗象信息科技有限公司	703
3	北京数字观星科技有限公司	8
4	中国电子科技网络信息安全有限公司	7
5	北京天地和兴科技有限公司	7
6	北京天融信网络安全技术有限公司	6
7	新华三技术有限公司	5
8	北京安信天行科技有限公司	3
9	上海安识网络科技有限公司	3
10	安徽长泰信息安全服务有限公司	2

11	北京智游网安科技有限公司	2
12	北京安帝科技有限公司 andisec 实验室	1
13	北京启明星辰信息安全技术有限公司	1
14	国网山西省电力公司电力科学研究院	1
15	湖南网鼎科技有限公司	1
16	信息工程大学	1
17	上海银基信息安全技术股份有限公司	1
报送总计		2642

三、接报漏洞预警情况

本周 CNNVD 接报漏洞预警 43 个。

序号	报送单位	漏洞总量
1	杭州迪普科技有限公司	14
2	北京启明星辰信息安全技术有限公司	5
3	北京华云安信息技术有限公司	4
4	北京天融信网络安全技术有限公司	4
5	知道创宇 404 实验室	3
6	深信服科技有限公司	3
7	杭州安恒信息技术股份有限公司	1
8	网神信息技术（北京）股份有限公司	1
9	北京神州绿盟科技有限公司安全研究部	1
10	新华三技术有限公司	1
11	杭州安恒信息技术股份有限公司	1
12	远江盛邦（北京）网络安全科技股份有限公司	1

13	北京长亭科技有限公司	1
14	北京山石网科信息技术有限公司	1
15	内蒙古洞明科技有限公司	1
16	北京圣博润高新技术股份有限公司	1
报送总计		43

四、重大漏洞预警

Apache Struts2 S2-059 安全漏洞预警

近日，国家信息安全漏洞库（CNNVD）收到关于 Apache Struts2 S2-059 安全漏洞（CNNVD-202008-743、CVE-2019-0230）情况的报送。成功利用漏洞的攻击者可能对目标系统执行恶意代码。Apache Struts 2.0.0 - Apache Struts 2.5.20 等版本均受此漏洞影响。目前，Apache 官方已经发布了版本更新修复了该漏洞。建议用户及时确认 Apache Struts 产品版本，如受影响，请及时采取修补措施。

.漏洞介绍

Apache Struts2 是美国阿帕奇（Apache）软件基金会下属的 Jakarta 项目中的一个子项目，是一个基于 MVC 设计的 Web 应用框架。

2020 年 8 月 13 日，Apache 官方发布安全公告，修复了一个远程代码执行漏洞，编号为 S2-059（CNNVD-202008-743、CVE-2019-0230）。该漏洞源于 Apache Struts 的框架在被强制使用时，会对标签的属性进行二次求值，最终导致远程代码执行。只有在 Struts 标签属性中

强制使用 OGNL 表达式时，才能触发漏洞。

.危害影响

成功利用该漏洞的攻击者，可以在目标系统中执行恶意代码。Apache Struts 2.0.0 - Apache Struts 2.5.20 等版本均受此漏洞影响。

.修复建议

目前，Apache 官方已经发布了版本更新修复了该漏洞。建议用户及时确认 Apache Struts 产品版本，如受影响，请及时采取修补措施。漏洞修补措施如下：

更新到 Struts 2.5.22 以上版本

http://struts.apache.org/download.cgi