信息安全漏洞周报

（2020 年第 48 期 总第 552 期）

信息安全测评中心　　2020 年 12 月 13 日

根据国家信息安全漏洞库（CNNVD）统计，本周（2020 年 12 月 07 日至 2020 年 12 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 510 个，与上周（171 个）相比增加了 198.25%。

接报漏洞情况

本周 CNNVD 接报漏洞 4304 个，其中信息技术产品漏洞（通用型漏洞）59 个，网络信息系统漏洞（事件型漏洞）4245 个。

重大漏洞预警

Apache Struts2 远程代码执行漏洞（CNNVD-202012-449、CVE-2020-17530）：成功利用漏洞的攻击者可以在目标系统执行恶意代码。Apache Struts 2.0.0 - 2.5.25 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。建议用户及时确认产品版本，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 510 个，漏洞新增数量有所上升。从厂商分布来看 Google 公司新增漏洞最多，有 126 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 7.65%。新增漏洞中，超危漏洞 52 个，高危漏洞 133 个，中危漏洞 305 个，低危漏洞 20 个。相应修复率分别为 80.77%、96.99%、90.49%和 95.00%。根据补丁信息统计，合计 466 个漏洞已有修复补丁发布，整体修复率为 91.37%。

（一） 安全漏洞增长数量情况

本周 CNNVD 采集安全漏洞 510 与上周（171 个）相比增多了 198.25%。

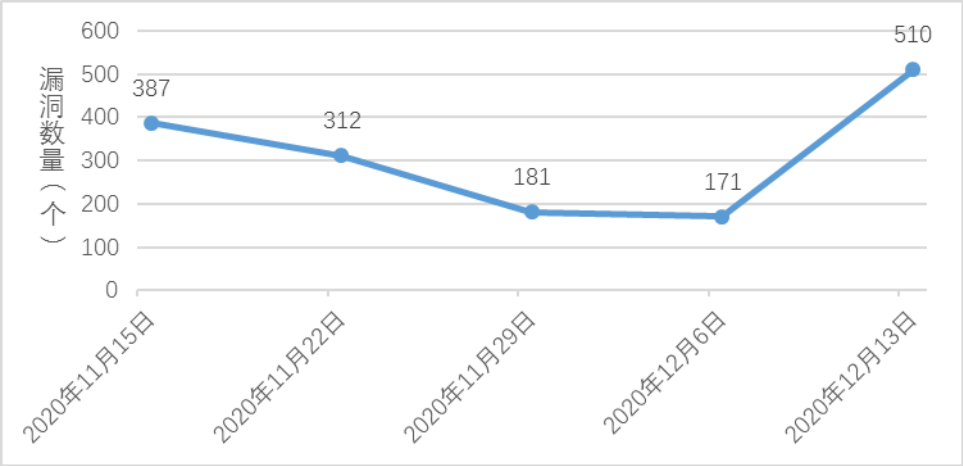

图 1 近五周漏洞新增数量统计图

（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 126 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	126	24.71%
2	Microsoft	60	11.76%
3	ImageMagick Studio	18	3.53%
4	Siemens	18	3.53%
5	Schneider Electric	17	3.33%

本周国内厂商漏洞 21 个，QNAP Systems 公司漏洞数量最多，有 8 个。国内厂商漏洞整体修复率为 95.24%。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 7.65%。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	39	7.65%
2	跨站脚本	39	7.65%
3	输入验证错误	34	6.67%
4	代码问题	26	5.10%
5	授权问题	23	4.51%
6	信息泄露	20	3.92%
7	资源管理错误	17	3.33%
8	访问控制错误	10	1.96%
9	代码注入	10	1.96%
10	SQL 注入	7	1.37%
11	注入	7	1.37%
12	权限许可和访问控制问题	3	0.59%
13	跨站请求伪造	3	0.59%
14	路径遍历	3	0.59%
15	操作系统命令注入	3	0.59%
16	命令注入	2	0.39%
17	数字错误	1	0.20%
18	数据伪造问题	1	0.20%
19	加密问题	1	0.20%
20	后置链接	1	0.20%
21	处理逻辑错误	1	0.20%

22	其他	256	50.20%

（三） 安全漏洞危害等级与修复情况

本周共发布超危漏洞 52 个，高危漏洞 133 个，中危漏洞 305 个，低危漏洞 20 个。相应修复率分别为 80.77%、96.99%、90.49%和 95.00%。根据补丁信息统计，合计 466 个漏洞已有修复补丁发布，整体修复率为 91.37%。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	52	42	80.77%
2	高危	133	129	96.99%
3	中危	305	276	90.49%
4	低危	20	19	95.00%
合计		510	466	91.37%

（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	代码注入	CNNVD-202012-606	Microsoft	Microsoft Exchange Server 代码注入漏洞	是	超危
2	其他	CNNVD-202012-449	Apache 基金会	Apache Struts 安全漏洞	是	高危
3	其他	CNNVD-202012-617	Microsoft	Microsoft SharePoint 安全漏洞	是	高危

1. Microsoft Exchange Server 代码注入漏洞（CNNVD-202012-606）

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 远程执行代码漏洞,目前尚无此漏洞的相关信息，请随时关注 CNNVD 或厂商公告。以下产品及版本受到影响:Microsoft Exchange Server 2016 Cumulative Update 17,Microsoft Exchange Server 2019 Cumulative Update 6,Microsoft Exchange Server 2013 Cumulative Update 23。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://msrc.microsoft.com/update-guide/zh-CN/vulnerability/CVE-2020-17142

2. Apache Struts 安全漏洞（CNNVD-202012-449）

Apache Struts 是美国阿帕奇（Apache）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。

Struts 存在安全漏洞，攻击者可利用该漏洞可以通过强迫 Struts 的 OGNL 评估来使用漏洞来运行代码。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://cwiki.apache.org/confluence/display/WW/S2-061

3. Microsoft SharePoint 安全漏洞（CNNVD-202012-617）

Microsoft SharePoint 是美国微软（Microsoft）公司的一套企业业务协作平台。该平台用于对业务信息进行整合,并能够共享工作、与他人协同工作、组织项目和工作组、搜索人员和信息。

Microsoft SharePoint 远程执行代码漏洞,目前尚无此漏洞的相关信息，请随时关注 CNNVD 或厂商公告。以下产品及版本受到影响:Microsoft SharePoint Enterprise Server 2016,Microsoft SharePoint Server 2019,Microsoft SharePoint Foundation 2010 Service Pack 2,Microsoft SharePoint Foundation 2013 Service Pack 1。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://msrc.microsoft.com/update-guide/zh-CN/vulnerability/CVE-2020-17121

二、接报漏洞情况

本周 CNNVD 接报漏洞 4304 个，其中信息技术产品漏洞（通用型漏洞）59 个，网络信息系统漏洞（事件型漏洞）4245 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	3334
2.	上海斗象信息科技有限公司	730
3.	山东云天安全技术有限公司	150
4.	广州竞远安全技术股份有限公司	16
5.	山东华鲁科技发展股份有限公司	15
6.	新华三技术有限公司	15
7.	北京数字观星科技有限公司	10
8.	北京华云安信息技术有限公司	7
9.	北京奇虎科技有限公司	4

10.	博智安全科技股份有限公司	4
11.	中兴通讯	3
12.	北京天融信网络安全技术有限公司	3
13.	苏州极光无限信息技术有限公司	3
14.	个人	2
15.	四川虹微技术有限公司	2
16.	信息工程大学	1
17.	内蒙古奥创科技有限公司	1
18.	北京智游网安科技有限公司	1
19.	北京计算机技术及应用研究所	1
20.	浙江大华技术股份有限公司	1
21.	湖南汽车工程职业学校	1
报送总计		4304

三、接报漏洞预警情况

本周 CNNVD 接报漏洞预警 69 个。

	报送单位	预警总量
1	深信服科技股份有限公司	16
2	杭州迪普科技股份有限公司	14
3	北京华云安信息技术有限公司	7
4	北京启明星辰信息安全技术有限公司	4
5	北京天融信网络安全技术有限公司	4
6	北京奇虎科技有限公司	3
7	新华三技术有限公司	3

8	杭州安恒信息技术股份有限公司	2
9	网神信息技术（北京）股份有限公司	2
10	北京知道创宇信息技术股份有限公司	2
11	北京华顺信安科技有限公司	2
12	浪潮电子信息产业股份有限公司	2
13	内蒙古洞明科技有限公司	2
14	北京神州绿盟科技有限公司	1
15	杭州安恒信息技术股份有限公司	1
16	远江盛邦(北京)网络安全科技股份有限公司	1
17	北京山石网科信息技术有限公司	1
18	上海斗像信息科技有限公司	1
19	亚信安全科技有限公司	1
报送总计		69

四、重大漏洞预警

Apache Struts 2 远程代码执行漏洞预警

近日，国家信息安全漏洞库（CNNVD）收到关于 Apache Struts2 S2-061 远程代码执行漏洞（CNNVD-202012-449、CVE-2020-17530）情况的报送。成功利用漏洞的攻击者可以在目标系统执行恶意代码。Apache Struts 2.0.0 - 2.5.25 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。建议用户及时确认产品版本，尽快采取修补措施。

.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。

洞源于 Apache Struts2 在某些标签属性中使用 OGNL 表达式时，因为没有做内容过滤，导致攻击者传入精心构造的请求时，可以造成 OGNL 二次解析，执行指定的恶意代码。

.危害影响

成功利用漏洞的攻击者可以在目标系统执行恶意代码。Apache Struts 2.0.0 - 2.5.25 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。建议用户及时确认产品版本，尽快采取修补措施。Apache 官方更新链接如下：

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