信息安全漏洞周报

（2020 年第 6 期 总第 510 期）

信息安全测评中心　　2020 年 2 月 16 日

根据国家信息安全漏洞库（CNNVD）统计，本周（2020 年 2 月 10 日至 2020 年 2 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 468 个，与上周（260 个）相比增加了 44.44%。

接报漏洞情况

本周 CNNVD 接报漏洞 829 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）802 个。

重大漏洞预警

微软多个安全漏洞：包括 Windows 远程执行代码漏洞（CNNVD-202002-510、CVE-2020-0662）、Windows LNK 远程执行代码漏洞（CNNVD-202002-544、CVE-2020-0729）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。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 468 个，漏洞新增数量有所上升。从厂商分布来看微软公司新增漏洞最多，有 100 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 15.17%。新增漏洞中，超危漏洞 40 个，高危漏洞 186 个，中危漏洞 215 个，低危漏洞 27 个。相应修复率分别为 65.00%、89.78%、67.44%和 88.89%。根据补丁信息统计，合计 362 个漏洞已有修复补丁发布，整体修复率为 77.35%。

（一） 安全漏洞增长数量情况

本周 CNNVD 采集安全漏洞 468 个，与上周（260 个）相比增加了 44.44%。图 1 为近五周漏洞新增数量统计图。

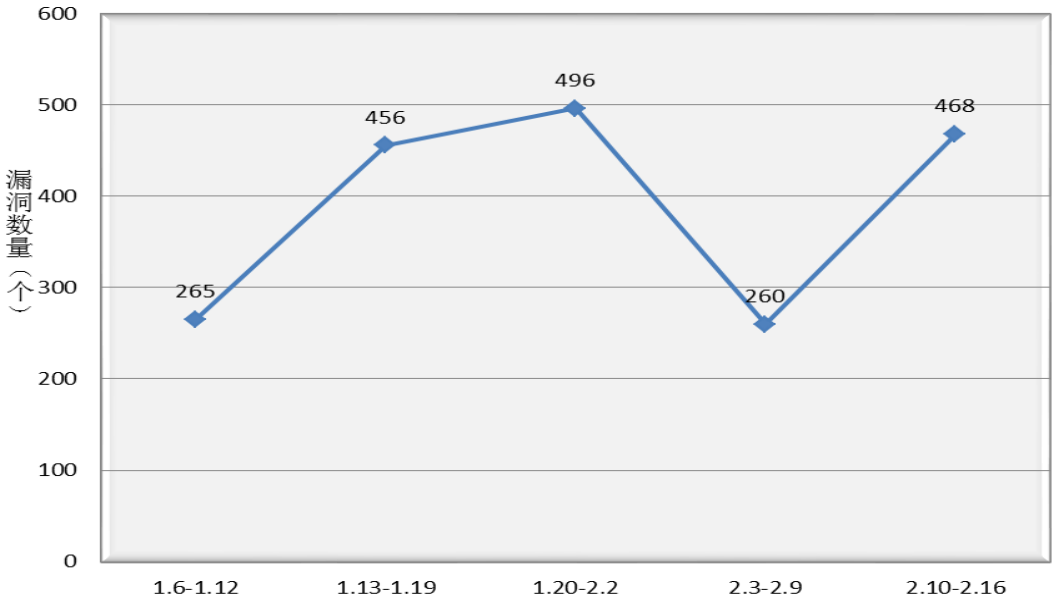

图 1 近五周漏洞新增数量统计图

（二） 安全漏洞分布情况

从厂商分布来看，微软公司新增漏洞最多，有 101 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	微软	101	21.58%
2	Adobe	42	8.97%
3	CloudBees	24	5.13%
4	福昕	14	2.99%
5	SAP	13	2.78%

本周国内厂商漏洞 19 个，福昕公司漏洞数量最多，有 14 个。国内厂商漏洞整体修复率为 94.73%。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 15.17%。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	71	15.17%
2	跨站脚本	43	9.19%
3	输入验证错误	17	3.63%
4	信息泄露	17	3.63%
5	跨站请求伪造	16	3.42%
6	代码问题	14	2.99%
7	资源管理错误	11	2.35%
8	授权问题	7	1.50%
9	SQL 注入	7	1.50%
10	注入	5	1.07%
11	操作系统命令注入	3	0.64%
12	路径遍历	3	0.64%
13	安全特征问题	1	0.21%
14	后置链接	1	0.21%
15	权限许可和访问控制问题	1	0.21%

16	加密问题	1	0.21%
17	命令注入	1	0.21%
18	代码注入	1	0.21%
19	信任管理问题	1	0.21%
20	访问控制错误	1	0.21%

（三） 安全漏洞危害等级与修复情况

本周共发布超危漏洞 40 个，高危漏洞 186 个，中危漏洞 215 个，低危漏洞 27 个。相应修复率分别为 65.00%、89.78%、67.44%和 88.89%。根据补丁信息统计，合计 362 个漏洞已有修复补丁发布，整体修复率为 77.35%。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	40	26	65.00%
2	高危	186	167	89.78%
3	中危	215	145	67.44%
4	低危	27	24	88.89%
合计		468	362	77.35%

（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	缓冲区错误	CNNVD-202002-625	Adobe	Adobe Framemaker 安全漏洞	是	超危
2	输入验证错误	CNNVD-202002-496	Microsoft	Microsoft SQL Server Reporting Services 输入验证错误漏洞	是	高危
3	其他	CNNVD-202002-817	Mozilla	Mozilla Firefox 和 Mozilla Firefox ESR 安全漏洞	是	高危

1. Adobe Framemaker 安全漏洞（CNNVD-202002-625）

Adobe FrameMaker 是一款系统应用软件。该软件是一款适用于 XML 和非结构化内容的创作和发布解决方案。

基于 Windows 平台的 Adobe Framemaker 2019.0.4 及之前版本中存在安全漏洞。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。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://helpx.adobe.com/security/products/framemaker/apsb20-04.html

2. Microsoft SQL Server Reporting Services 输入验证错误漏洞（CNNVD-202002-496）

Microsoft SQL Server Reporting Services（SSRS）是美国微软（Microsoft）公司的一套基于服务器的报告平台，它支持创建、部署和管理移动和分页报表。

Microsoft SQL Server Reporting Services 中存在远程代码执行漏洞，该漏洞源于程序不正确的处理页面请求。攻击者可利用该漏洞在系统上执行代码。以下产品及版本受到影响：Microsoft SQL Server 2012，Microsoft SQL Server 2014 Service Pack 3，Microsoft SQL Server 2016。

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-2020-0618

3. Mozilla Firefox 和 Mozilla Firefox ESR 安全漏洞

（CNNVD-202002-817）

Mozilla Firefox 和 Mozilla Firefox ESR 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。

基于 Windows 平台的 Mozilla Firefox 73 之前版本和 Firefox ESR 68.5 之前版本中存在安全漏洞。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.mozilla.org/en-US/security/advisories/mfsa2020-05/

https://www.mozilla.org/en-US/security/advisories/mfsa2020-06/

二、接报漏洞情况

本周 CNNVD 接报漏洞 829 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）802 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	133
3	内蒙古洞明科技有限公司	99
4	北京华云安信息技术有限公司	39
5	太极计算机股份有限公司	20

6	北京圣溥润高新技术服份有限公司	9
7	国发中新（北京）科技发展有限公司	5
8	北京启明星辰信息安全技术有限公司	3
报送总计		829

三、重大漏洞预警

微软多个安全漏洞预警

近日，微软官方发布了用于修复 101 个安全漏洞的公告，包括 Windows 远程执行代码漏洞（CNNVD-202002-510、CVE-2020-0662）、Windows LNK 远程执行代码漏洞（CNNVD-202002-544、CVE-2020-0729）、Microsoft Internet Explorer 内存破坏漏洞（CNNVD-202001-876、CVE-2020-0674）；Windows 远程桌面客户端远程代码执行漏洞（CNNVD-202002-541、CVE-2020-0681；CNNVD-202002-538、CVE-2020-0734；CNNVD-202002-646、CVE-2020-0817）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

本次漏洞公告涉及 Windows 操作系统、Microsoft Office、Edge、Internet Explorer、Microsoft Exchange Server、Microsoft Surface Hub、ChakraCore 等 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，漏洞详情如下：

1、Windows 远程执行代码漏洞（CNNVD-202002-510、CVE-2020-0662）

漏洞简介：Windows 无法正确处理内存中的对象时，会触发一个远程代码执行漏洞。成功利用此漏洞的攻击者可以通过提升权限在目标系统上执行任意代码。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。

2、Windows LNK 远程执行代码漏洞（CNNVD-202002-544、CVE-2020-0729）

漏洞简介：Microsoft Windows 在处理.LNK 文件过程中存在一个远程执行代码漏洞。成功利用此漏洞的攻击者可能会获得与本地用户相同的用户权限。攻击者可能会向用户发送包含恶意 .LNK 文件和关联的恶意二进制文件的可移除驱动器或远程共享。当用户在 Windows 资源管理器中打开此驱动器（或远程共享），或打开可分析 .LNK 文件的其他任何应用程序时，攻击者即可在目标系统上执行代码。

3、Microsoft Internet Explorer 内存破坏漏洞（CNNVD-202001-876、CVE-2020-0674）

漏洞简介：当 Internet Explorer 不正确地访问内存中的对象时，会触发一个远程代码执行漏洞。该漏洞可以使攻击者在当前用户的上下文中执行任意代码，以此来破坏内存。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。

4、Windows 远程桌面客户端远程代码执行漏洞（CNNVD-202002-541、CVE-2020-0681 ； CNNVD-202002-538 、 CVE-2020-0734 ； CNNVD-202002-646、CVE-2020-0817）

漏洞简介： Windows 远程桌面客户端中存在多个远程代码执行漏洞，当用户连接到恶意服务器时，会触发该漏洞。成功利用此漏洞的攻击者可以在连接客户端的计算机中执行任意代码，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。

5 、 Media Foundation 内 存 破 坏 漏 洞 （ CNNVD-202002-528 、CVE-2020-0738）

漏洞简介：当 Windows Media Foundation 不正确地访问内存中的对象时，会触发一个远程代码执行漏洞。该漏洞可以使攻击者在当前用户的上下文中执行任意代码，以此来破坏内存。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。

6、Microsoft ChakraCore 和 Edge 内存破坏漏洞(CNNVD-202002-579、CVE-2020-0710 ； CNNVD-202002-566 、 CVE-2020-0711 ；

CNNVD-202002-580 、 CVE-2020-0712 ； CNNVD-202002-572 、 CVE-2020-0713）

漏洞简介：Microsoft Edge (EdgeHTML-based)和 ChakraCore 中存在远程执行代码漏洞。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。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 Excel 资源管理错误漏洞（CNNVD-202002-585、CVE-2020-0759）

漏洞简介：Microsoft Excel 中存在资源管理错误漏洞，该漏洞源于该软件没有正确处理内存中的对象。攻击者可利用该漏洞在当前用户的上下文中运行任意代码。攻击者可利用漏洞安装程序；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。

8、Microsoft SQL Server 和 Microsoft SQL Server Reporting Services 远程执行代码漏洞（CNNVD-202002-496、CVE-2020-0618）

漏洞简介：当 Microsoft SQL Server 和 Microsoft SQL Server Reporting Services 错误地处理页面请求时，会触发一个远程代码执行漏洞。成功利用该漏洞的攻击者会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用户权限登录，那么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。

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	Windows 远程执行代码漏洞（CNNVD-202002-510、CVE-2020-0662）	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-0662
2	Windows LNK 远程执行代码漏洞（CNNVD-202002-544、CVE-2020-0729）	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-0729
3	Microsoft Internet Explorer 内存破坏漏洞（CNNVD-202001-876、CVE-2020-0674）	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-0674
4	Windows 远程桌面客户端远程代码执行漏洞（CNNVD-202002-541、CVE-2020-0681；CNNVD-202002-538、CVE-2020-0734；CNNVD-202002-646、CVE-2020-0817）	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-0681 https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-0734 https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-0817
5	Media Foundation 内存破坏漏洞（CNNVD-202002-528、CVE-2020-0738）	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-0738
6	Microsoft ChakraCore 和 Edge 内存破坏漏洞（CNNVD-202002-579、CVE-2020-0710；CNNVD-202002-566、CVE-2020-0711；CNNVD-202002-580、CVE-2020-0712；CNNVD-202002-572、CVE-2020-0713）	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-0710 https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-0711 https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-0712 https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-0713
7	Microsoft Excel 资源管理错误漏洞	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-0759

	（ CNNVD-202002-585 、CVE-2020-0759）	
8	Microsoft SQL Server 和 Microsoft SQL Server Reporting Services 远程执行代码漏洞（ CNNVD-202002-496 、CVE-2020-0618）	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-0618