信息安全漏洞周报

（2020 年第 8 期 总第 512 期）

信息安全测评中心　　2020 年 3 月 2 日

根据国家信息安全漏洞库（CNNVD）统计，本周（2020 年 2 月 24 日至 2020 年 3 月 1 日）安全漏洞情况如下：

公开漏洞情况

本周 CNNVD 采集安全漏洞 215 个，与上周（241 个）相比减少了 10.78%。

接报漏洞情况

本周 CNNVD 接报漏洞 1230 个，其中信息技术产品漏洞（通用型漏洞）83 个，网络信息系统漏洞（事件型漏洞）1147 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 215 个，漏洞新增数量有所上升。从厂商分布来看 Moxa 公司新增漏洞最多，有 36；从漏洞类型来看，跨站脚本类的安全漏洞占比最大，达到 10.70%。新增漏洞中，超危漏洞 42 个，高危漏洞 70 个，中危漏洞 99 个，低危漏洞 4 个。相应修复率分别为 85.71%、77.14%、74.75%和 100.00%。根据补丁信息统计，合计 168 个漏洞已有修复补丁发布，整体修复率为 78.14%。

（一） 安全漏洞增长数量情况

本周 CNNVD 采集安全漏洞 215 个，与上周（241 个）相比减少了 10.78%。图 1 为近五周漏洞新增数量统计图。

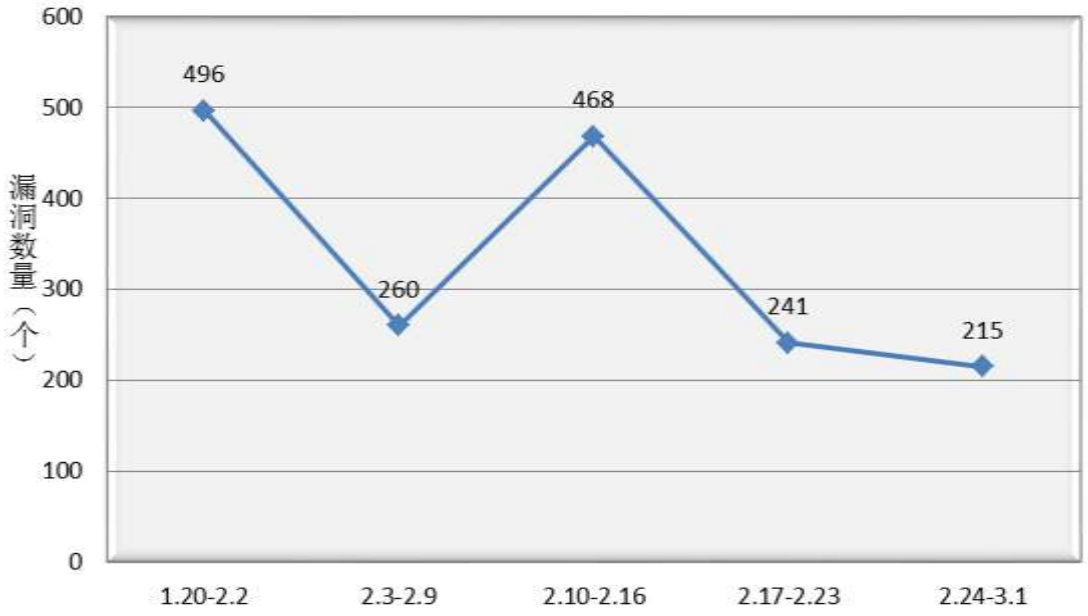

图 1 近五周漏洞新增数量统计图

（二） 安全漏洞分布情况

从厂商分布来看，Moxa 公司新增漏洞最多，有 36 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	摩莎	36	16.74%
2	IBM	12	5.58%
3	思科	11	5.12%
4	Selesta Ingegneria	9	4.19%
5	谷歌	6	2.79%

本周国内厂商漏洞 46 个，摩莎公司漏洞数量最多，有 36 个。国内厂商漏洞整体修复率为 91.30%。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 10.70%。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	23	10.70%
2	缓冲区错误	15	6.98%
3	操作系统命令注入	13	6.05%
4	注入	10	4.65%
5	信息泄露	10	4.65%
6	信任管理问题	8	3.72%
7	跨站请求伪造	8	3.72%
8	输入验证错误	7	3.26%
9	SQL 注入	7	3.26%
10	资源管理错误	6	2.79%
11	代码问题	5	2.33%
12	路径遍历	5	2.33%
13	授权问题	4	1.86%
14	命令注入	3	1.40%
15	访问控制错误	3	1.40%
16	数据伪造问题	2	0.93%
17	环境问题	1	0.47%
18	格式化字符串错误	1	0.47%

19	代码注入	1	0.47%
20	加密问题	1	0.47%
21	数字错误	1	0.47%
22	其他	81	37.67%

（三） 安全漏洞危害等级与修复情况

本周共发布超危漏洞 42 个，高危漏洞 70 个，中危漏洞 99 个，低危漏洞 4 个。相应修复率分别为 85.71%、77.14%、74.75%和 100.00%。根据补丁信息统计，合计 168 个漏洞已有修复补丁发布，整体修复率为 78.14%。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	42	36	85.71%
2	高危	70	54	77.14%
3	中危	99	74	74.75%
4	低危	4	4	100.00%
合计		215	168	78.14%

（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-202002-1161	摩莎	Moxa EDS-G516E 和 EDS-510E 缓冲区错误漏洞	是	超危
2	缓冲区错误	CNNVD-202002-1192	谷歌	Google Chrome 缓冲区错误漏洞	是	高危
3	路径遍历	CNNVD-202002-1104	DNN	DNN 路径遍历漏洞	是	高危

1. Moxa EDS-G516E 和 EDS-510E 缓冲区错误漏洞

（CNNVD-202002-1161）

Moxa EDS-G516E 和 EDS-510E 都是中国台湾摩莎（Moxa）公司的管理型交换机。

使用 5.2 及之前版本固件的 Moxa EDS-G516E 系列和 EDS-510E 系列存在缓冲区错误漏洞，该漏洞源于程序允许用户使用较弱的密码。攻击者可利用该漏洞入侵用户账户。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://www.moxa.com/en/support/support/security-advisory/eds-g516e-510e-ethernet-switches-vulnerabilities

2. Google Chrome 缓冲区错误漏洞（CNNVD-202002-1192）

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

Google Chrome 80.0.3987.122 之前版本中存在安全漏洞。远程攻击者可借助特制的网站利用该漏洞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://chromereleases.googleblog.com/2020/02/stable-channel-update-for-desktop_24.html

3. DNN 路径遍历漏洞（CNNVD-202002-1104）

DNN（又名 DotNetNuke）是美国 DNN 公司的一套由微软支持、基于 ASP.NET 平台的开源内容管理系统（CMS）。该系统具有易于安装、可扩展、功能丰富等特点。

DNN 9.4.4 及之前版本中存在路径遍历漏洞。该漏洞源于网络系统或产品未能正确地过滤资源或文件路径中的特殊元素。攻击者可利

用该漏洞访问受限目录之外的位置。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://github.com/dnnsoftware/Dnn.Platform/releases

二、接报漏洞情况

本周 CNNVD 接报漏洞 1230 个，其中信息技术产品漏洞（通用型漏洞）83 个，网络信息系统漏洞（事件型漏洞）1147 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	407
2	上海斗象信息科技有限公司	345
3	内蒙古洞明科技有限公司	159
4	北京华云安信息技术有限公司	75
5	太极计算机股份有限公司	65
6	山东新潮信息技术有限公司	52
7	北京圣溥润高新技术服份有限公司	26
8	西安四叶草信息技术有限公司	20
9	浙江大华技术股份有限公司	12
10	深信服电子科技有限公司	10
11	北京数字观星科技有限公司	10
12	北京云测信息技术有限公司	8
13	个人	7
14	国防科技大学	6
15	上海安识网络科技有限公司	4

16	北京国舜科技股份有限公司	4
17	北京圣博润高新技术股份有限公司	3
18	西安交大捷普网络科技有限公司	2
19	北京云测信息科技有限公司	2
20	北京神州绿盟科技有限公司工业物联网安全实验室	2
21	北京山石网科信息技术有限公司	2
22	中国工商银行安全攻防实验室	1
23	上海安几科技有限公司	1
24	北京智游网安科技有限公司	1
25	北京长亭未来科技有限公司	1
26	北京长亭科技有限公司	1
27	北京邮电大学	1
28	北京神州绿盟科技有限公司网络攻防实验室	1
29	北京神州绿盟科技有限公司安全研究部	1
30	北京国舜科技股份有限公司、华北技术服务中心、安全工程师	1
报送总计		1230