信息安全漏洞周报

（2021 年第 4 期 总第 558 期）

信息安全测评中心　　2020 年 1 月 24 日

根据国家信息安全漏洞库（CNNVD）统计，本周（2021 年 1 月 18 日至 2021 年 1 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 359 个，与上周（473 个）相比减少了 24.10%。

接报漏洞情况

本周 CNNVD 接报漏洞 2963 个，其中信息技术产品漏洞（通用型漏洞）367 个，网络信息系统漏洞（事件型漏洞）2596 个。

重大漏洞预警

Dnsmasq 多个缓冲区错误漏洞的预警（CNNVD-202101-1570、CVE-2020-25681）（CNNVD-202101-1569、CVE-2020-25682）：成功利用漏洞的攻击者，可进行内存破坏、拒绝服务等攻击，甚至可以远程执行恶意代码，最终控制目标服务器。Dnsmsaq 2.83 以下版本均受漏洞影响。目前，Dnsmasq 官方已经发布了升级补丁修复了该漏洞，建议用户及时确认版本信息，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 359 个，漏洞新增数量有所下降。从厂商分布来看思科公司新增漏洞最多，有 58 个；从漏洞类型来看，访问控制错误类的安全漏洞占比最大，达到 13.37%。新增漏洞中，超危漏洞 30 个，高危漏洞 130 个，中危漏洞 189 个，低危漏洞 10 个。相应修复率分别为 93.33%、95.38%、93.65%和 90.00%。根据补丁信息统计，合计 338 个漏洞已有修复补丁发布，整体修复率为 94.15%。

（一） 安全漏洞增长数量情况

本周 CNNVD 采集安全漏洞 359 与上周（473 个）相比减少了 24.10%。

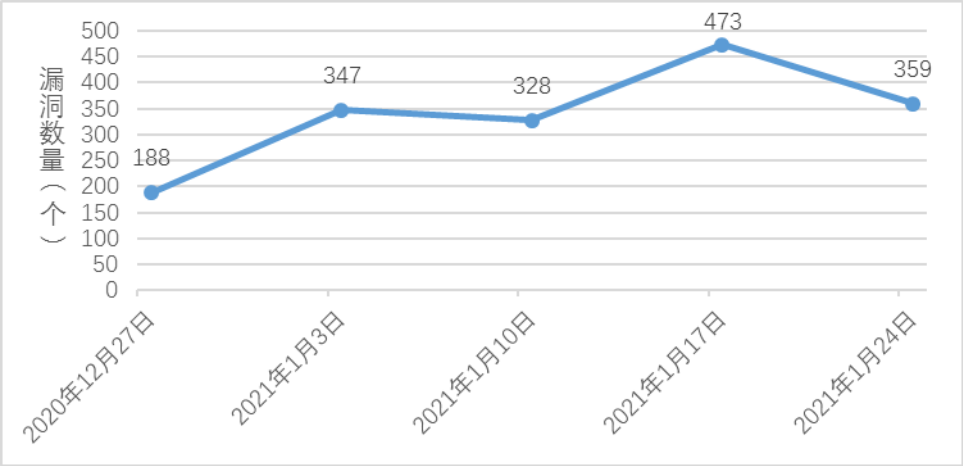

图 1 近五周漏洞新增数量统计图

（二） 安全漏洞分布情况

从厂商分布来看，思科公司新增漏洞最多，有 58 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	思科	58	16.16%
2	谷歌	25	6.96%
3	IBM	12	3.34%
4	NEC	4	1.11%
5	Honeywell	4	1.11%

本周国内厂商漏洞 7 个，华为公司和慧远公司漏洞数量最多，各有 2 个。国内厂商漏洞整体修复率为 87.50%。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，访问控制错误类和授权问题类的安全漏洞占比最大，均达到 13.37%。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	访问控制错误	48	13.37%
2	授权问题	48	13.37%
3	输入验证错误	23	6.41%
4	跨站脚本	22	6.13%
5	代码问题	17	4.74%
6	缓冲区错误	16	4.46%
7	信息泄露	15	4.18%
8	SQL 注入	10	2.79%
9	跨站请求伪造	6	1.67%
10	资源管理错误	5	1.39%
11	路径遍历	5	1.39%
12	命令注入	3	0.84%
13	信任管理问题	3	0.84%
14	安全特征问题	3	0.84%
15	注入	2	0.56%
16	数据伪造问题	2	0.56%
17	加密问题	1	0.28%
18	操作系统命令注入	1	0.28%
19	其他	127	35.38%

（三） 安全漏洞危害等级与修复情况

本周共发布超危漏洞 30 个，高危漏洞 130 个，中危漏洞 189 个，低危漏洞 10 个。相应修复率分别为 93.33%、95.38%、93.65%和 90.00%。根据补丁信息统计，合计 338 个漏洞已有修复补丁发布，整体修复率为 94.15%。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	30	28	93.33%
2	高危	130	124	95.38%
3	中危	189	177	93.65%
4	低危	10	9	90.00%
合计		359	338	94.15%

（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	授权问题	CNNVD-202101-1326	Oracle	Oracle Fusion Middleware 授权问题漏洞	是	超危
2	SQL 注入	CNNVD-202101-1513	Cisco	Cisco Data Center Network Manager SQL 注入漏洞	是	高危
3	资源管理错误	CNNVD-202101-1580	Google	Google Chrome 资源管理错误漏洞	是	高危

1. Oracle Fusion Middleware 授权问题漏洞（CNNVD-202101-1326）

Oracle Fusion Middleware（Oracle 融合中间件）是美国甲骨文（Oracle）公司的一套面向企业和云环境的业务创新平台。该平台

提供了中间件、软件集合等功能。

Oracle Fusion Middleware 的 Oracle Coherence product 组件存在授权问题漏洞，该漏洞允许未经身份验证的攻击者通过 IIOP、T3 进行网络访问，从而破坏 Oracle Coherence。以下产品及版本受到影响：3.7.1.0、12.1.3.0.0、12.2.1.3.0、12.2.1.4.0 和 14.1.1.0.0。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://www.oracle.com/security-alerts/cpujan2021.html

2. Cisco Data Center Network Manager SQL 注入漏洞（CNNVD-202101-1513）

Cisco Data Center Network Manager（DCNM）是美国思科（Cisco）公司的一套数据中心管理系统。该系统适用于 Cisco Nexus 和 MDS 系列交换机，提供存储可视化、配置和故障排除等功能。

Cisco Data Center Network Manager 存在安全漏洞，该漏洞允许经过身份验证的远程攻击者在受影响的设备上执行任意 SQL 命令。

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-dcnm-sql-inj-OAQOObP

3. Google Chrome 资源管理错误漏洞（CNNVD-202101-1580）

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

Google Chrome 存在资源管理错误漏洞，该漏洞源于 Google Chrome 在使用 DevTools 组件时不受限制而导致触发漏洞。

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/2021/01/stable-channel-update-for-desktop_19.html

二、接报漏洞情况

本周 CNNVD 接报漏洞 2963 个，其中信息技术产品漏洞（通用型漏洞）367 个，网络信息系统漏洞（事件型漏洞）2596 个。

表 5 本周漏洞报送情况

序号	报送单位	漏洞总量
1	上海斗像信息科技有限公司	1164
2	网神信息技术（北京）股份有限公司	745
3	北京数字观星科技有限公司	473
4	北京山石网科信息技术有限公司	124
5	山东新潮信息技术有限公司	88
6	西安四叶草信息技术有限公司	60
7	西安交大捷普网络科技有限公司	49
8	北京天地和兴科技有限公司	44
9	北京顶象技术有限公司洞见安全实验室	36
10	山东华鲁科技发展股份有限公司	30
11	安徽长泰信息安全服务有限公司	22
12	华为技术有限公司未然实验室	19
13	北京启明星辰信息安全技术有限公司	15
14	杭州默安科技有限公司	11
15	北京赋云安运营科技有限公司	10
16	安徽华云网安信息技术有限公司	10

17	湖南匡安网络技术有限公司	10
18	杭州安恒信息技术股份有限公司	8
19	广州竞远安全技术股份有限公司	6
20	深信服科技股份有限公司	6
21	北京云测信息技术有限公司	4
22	山东云天安全技术有限公司	4
23	北京时代新威信息技术有限公司	3
24	北京圣博润高新技术股份有限公司	3
25	四川虹微技术有限公司	3
26	博智安全科技股份有限公司	2
27	中电长城网际系统应用有限公司	2
28	北京天融信网络安全技术有限公司	2
29	广东网安科技有限公司	2
30	中国信息安全测评中心华中测评中心	1
31	个人	1
32	中兴通讯股份有限公司沉烽实验室	1
33	北京安帝科技有限公司	1
34	北京时代新威信息技术有限公司	1
35	北京智游网安科技有限公司	1
36	嘀嗒出行	1
37	长扬科技(北京)有限公司	1
报送总计		2963

三、接报漏洞预警情况

本周 CNNVD 接报漏洞预警 79 份。

序号	报送单位	预警总量
1	深信服科技股份有限公司	22
2	北京天融信网络安全技术有限公司	14
3	北京华云安信息技术有限公司	7
4	北京奇虎科技有限公司	5
5	北京启明星辰信息安全技术有限公司	4
6	浪潮电子信息产业股份有限公司	4
7	北京华顺信安科技有限公司	3
8	内蒙古奥创科技有限公司	3
9	北京知道创宇信息技术股份有限公司	2
10	北京中测安华科技有限公司	2
11	华为技术有限公司未然实验室	2
12	新华三技术有限公司	2
13	长扬科技（北京）有限公司	2
14	博智安全科技股份有限公司	2
15	北京山石网科信息技术有限公司	1
16	杭州安恒信息技术股份有限公司	1
17	内蒙古洞明科技有限公司	1
18	网神信息技术（北京）股份有限公司	1
19	远江盛邦(北京)网络安全科技股份有限公司	1
报送总计		79

四、重大漏洞预警

Dnsmasq 多个缓冲区错误漏洞的预警

近日，国家信息安全漏洞库（CNNVD）收到 2 个 Dnsmasq 缓冲区错误漏洞（CNNVD-202101-1570、CVE-2020-25681）（CNNVD-202101-1569、CVE-2020-25682）情况的报送。成功利用漏洞的攻击者，可进行内存破坏、拒绝服务等攻击，甚至可以远程执行恶意代码，最终控制目标服务器。Dnsmsaq 2.83 以下版本均受漏洞影响。目前，Dnsmasq 官方已经发布了升级补丁修复了该漏洞，建议用户及时确认版本信息，尽快采取修补措施。

.漏洞介绍

Dnsmasq 是一款使用 C 语言编写的轻量级 DNS 转发和 DHCP、TFTP 服务器。

漏洞源于 Dnsmasq 处理代码的边界检查错误，当 Dnsmasq 开启了“DNSSEC”特性后，攻击者可利用此漏洞将任意数据写入目标设备的内存中，导致目标设备上的内存损坏，影响 DNS 服务正常的运行，造成拒绝服务或远程代码执行。

.危害影响

成功利用漏洞的攻击者，可进行内存破坏、拒绝服务等攻击，甚至可以远程执行恶意代码，最终控制目标服务器。Dnsmsaq 2.83 以下版本均受漏洞影响。

Dnsmasq 在全球范围内有多家企业使用，其中至少包括了 Arista Networks Inc、Cradlepoint、Digi International、安卓、康卡斯特、思科、红帽、Netgear、高通、Linksys、IBM、西门子、Pi-Hole、友讯、戴尔、华为、优倍快等　。通过网络测绘系统发现，全球超过 130 万个 Dnsmasq 服务器使用记录，其中中国排名第一，共 98 万条记录，美国第二，共 28 万条记录。

.修复建议

目前，Dnsmasq 官方已经发布了升级补丁修复了该漏洞，建议用户及时确认版本信息，尽快采取修补措施。Dnsmasq 官方更新链接如下：

https://www.jsof-tech.com/disclosures/dnspooq/