北京师范大学网络信息安全通告

2022 年 3 月报告

北京师范大学信息网络中心

2022 年 4 月

目录

漏洞态势

一、公开漏洞情况

根据国家信息安全漏洞库（CNNVD）统计，2022 年 3 月份新增安全漏洞共 2065 个，从厂商分布来看，Google 公司产品的漏洞数量最多，共发布 165 个；从漏洞类型来看，跨站脚本类的漏洞占比最大，达到 13.41%。本月新增漏洞中，超危漏洞 373 个、高危漏洞 709 个、中危漏洞 929 个、低危漏洞 54 个，相应修复率分别为 64.88%、81.52%、77.72%以及 87.04%。合计 1589 个漏洞已有修复补丁发布，本月整体修复率 76.95%。

截至 2022 年 03 月 31 日，CNNVD 采集漏洞总量已达 180642 个。

1.1 漏洞增长概况

2022 年 3 月新增安全漏洞 2065 个，与上月（1859 个）相比增加了 11.08%。根据近 6 个月来漏洞新增数量统计图，平均每月漏洞数量达到 1895 个。

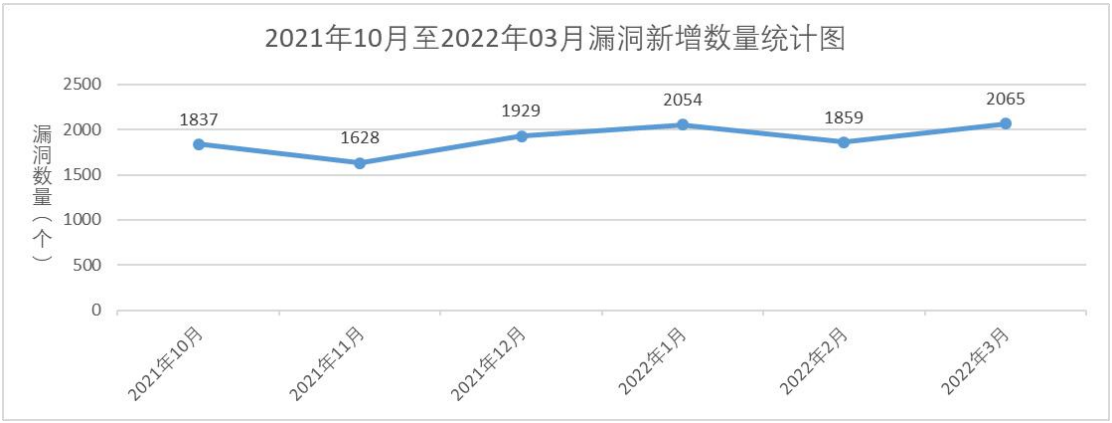

图 1 2021 年 10 月至 2022 年 3 月漏洞新增数量统计图

1.2 漏洞分布情况

1.2.1 漏洞厂商分布

2022 年 3 月厂商漏洞数量分布情况如表 1 所示，Google 公司漏洞达到 165 个，占本月漏洞总量的 7.99%。

表 1　2022 年 3 月排名前十厂商新增安全漏洞统计表

序号	厂商名称	漏洞数量（个）	所占比例
1	Google	165	7.99%
2	WordPress 基金会	158	7.65%
3	Microsoft	71	3.44%
4	Apple	69	3.34%
5	Tenda	64	3.10%
6	Linux 基金会	36	1.74%
7	IBM	28	1.36%
8	HP	21	1.02%
9	Siemens	20	0.97%
10	Samsung	20	0.97%

1.2.2 漏洞产品分布

2022 年 3 月主流操作系统的漏洞统计情况如表 2 所示。本月 Windows 系列操作系统漏洞数量共 33 个[1]，Android 漏洞数量最多，共 109 个，占主流操作系统漏洞总量的 27.05%，排名第一。

表 2　2022 年 3 月主流操作系统漏洞数量统计

序号	操作系统名称	漏洞数量
1	Android	109
2	Windows 10	32
3	Windows Server 2022	29
4	Windows Server 2019	29
5	Windows 11	28
6	Windows Server 2016	26

[1] Windows 系列操作系统多个版本可能同时受同一个漏洞影响。

7	Windows Server 2012	23
8	Windows Server 2012 R2	23
9	Windows 8.1	23
10	Windows Rt 8.1	22
11	Windows 7	16
12	Windows Server 2008	15
13	Windows Server 2008 R2	15
14	Linux Kernel	13

1.2.3 漏洞类型分布

2022 年 3 月份发布的漏洞类型分布如表 3 所示，其中跨站脚本类漏洞所占比例最大，约为 13.41%。

表 3 2022 年 3 月漏洞类型统计表

序号	漏洞类型	漏洞数量（个）	所占比例
1	跨站脚本	277	13.41%
2	缓冲区错误	208	10.07%
3	SQL 注入	120	5.81%
4	代码问题	116	5.62%
5	输入验证错误	81	3.92%
6	资源管理错误	79	3.83%
7	信息泄露	65	3.15%
8	权限许可和访问控制问题	59	2.86%
9	代码注入	59	2.86%
10	命令注入	58	2.81%
11	访问控制错误	49	2.37%
12	授权问题	49	2.37%
13	路径遍历	44	2.13%
14	操作系统命令注入	41	1.99%
15	跨站请求伪造	39	1.89%
16	安全特征问题	19	0.92%
17	竞争条件问题	17	0.82%
18	信任管理问题	16	0.77%
19	数据伪造问题	11	0.53%
20	日志信息泄露	8	0.39%
21	加密问题	7	0.34%
22	注入	6	0.29%
23	数字错误	6	0.29%

24	环境问题	4	0.19%
25	后置链接	3	0.15%
26	参数注入	2	0.10%
27	格式化字符串错误	1	0.05%
28	其他	621	30.07%

1.2.4 漏洞危害等级分布

根据漏洞的影响范围、利用方式、攻击后果等情况，从高到低可将其分为四个危害等级，即超危、高危、中危和低危级别。2022 年 3 月漏洞危害等级分布如图 2 所示，其中超危漏洞 373 条，占本月漏洞总数的 18.06%。

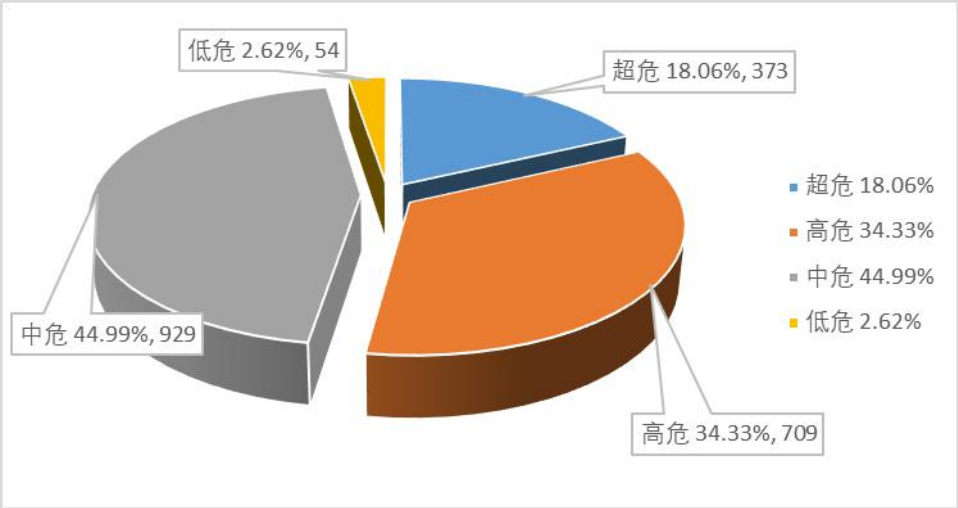

图 2　2022 年 3 月漏洞危害等级分布

1.3 漏洞修复情况

1.3.1 整体修复情况

2022 年 3 月漏洞修复情况按危害等级进行统计见图 3。其中低危漏洞修复率最高，达到 87.04%，超危漏洞修复率最低，比例为 64.88%。

总体来看，本月整体修复率，由上月的 89.73%下降至本月的 76.95%。

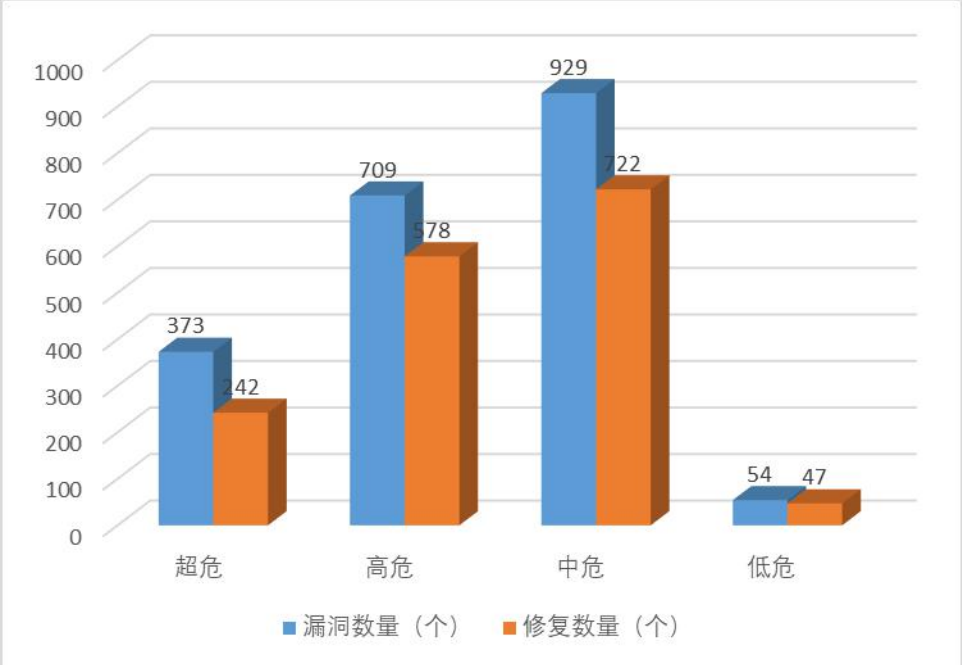

图 3　2022 年 3 月漏洞修复数量统计

1.3.2 厂商修复情况

2022 年 3 月漏洞修复情况按漏洞数量前十厂商进行统计，其中 Google、WordPress 基金会、Microsoft 等十个厂商共 652 条漏洞，占本月漏洞总数的 31.57%，漏洞修复率为 92.18%，详细情况见表 4。多数知名厂商对产品安全高度重视，产品漏洞修复比较及时，其中 Google、Microsoft、HP、Siemens、Samsung 等公司本月漏洞修复率均为 100%，共 601 条漏洞已全部修复。

表 4　2022 年 3 月厂商修复情况统计表

序号	厂商名称	漏洞数量（个）	修复数量	修复率
1	Google	165	165	100.00%
2	WordPress 基金会	158	152	96.20%
3	Microsoft	71	71	100.00%

4	Apple	69	68	98.55%
5	Tenda	64	31	48.44%
6	Linux 基金会	36	29	80.56%
7	IBM	28	24	85.71%
8	HP	21	21	100.00%
9	Siemens	20	20	100.00%
10	Samsung	20	20	100.00%

1.4 重要漏洞实例

1.4.1 超危漏洞实例

2022 年 3 月超危漏洞共 374 个，其中重要漏洞实例如表 5 所示。

表 5　2022 年 3 月超危漏洞实例

漏洞类型	厂商	CNNVD 编号	漏洞实例
SQL 注入	Apache 基金会	CNNVD-202203-1999	Rapid7 Nexpose SQL 注入漏洞（CNNVD-202203-1606）
	Delta	CNNVD-202203-1987	
		CNNVD-202203-1989	
		CNNVD-202203-1990	
		CNNVD-202203-1993	
		CNNVD-202203-1995	
		CNNVD-202203-1997	
		CNNVD-202203-2001	
		CNNVD-202203-2002	
		CNNVD-202203-2003	
		CNNVD-202203-2005	
		CNNVD-202203-2006	
		CNNVD-202203-2008	
		CNNVD-202203-2009	
		CNNVD-202203-2011	
		CNNVD-202203-2013	
	MingSoft	CNNVD-202203-152	
		CNNVD-202203-153	
		CNNVD-202203-155	
	Rapid7	CNNVD-202203-1606	
	Softwell	CNNVD-202203-1992	
	SourceCodester	CNNVD-202203-1556	
		CNNVD-202203-1959	
	WordPress 基金会	CNNVD-202203-601	

		CNNVD-202203-610	
		CNNVD-202203-1312	
		CNNVD-202203-1328	
		CNNVD-202203-1332	
		CNNVD-202203-1343	
		CNNVD-202203-1907	
		CNNVD-202203-1909	
		CNNVD-202203-1910	
		CNNVD-202203-1911	
	个人开发者	CNNVD-202203-105	
		CNNVD-202203-111	
		CNNVD-202203-112	
		CNNVD-202203-113	
		CNNVD-202203-114	
		CNNVD-202203-116	
		CNNVD-202203-117	
		CNNVD-202203-457	
		CNNVD-202203-904	
		CNNVD-202203-905	
		CNNVD-202203-906	
		CNNVD-202203-907	
		CNNVD-202203-908	
		CNNVD-202203-909	
		CNNVD-202203-910	
		CNNVD-202203-1351	
		CNNVD-202203-1437	
		CNNVD-202203-1464	
		CNNVD-202203-1466	
		CNNVD-202203-1471	
		CNNVD-202203-1472	
		CNNVD-202203-1602	
		CNNVD-202203-1887	
		CNNVD-202203-1957	
		CNNVD-202203-1960	
		CNNVD-202203-2004	
		CNNVD-202203-2037	
		CNNVD-202203-2050	
		CNNVD-202203-2118	
		CNNVD-202203-2134	
		CNNVD-202203-2143	
		CNNVD-202203-2297	
		CNNVD-202203-2309	
代码问题	Apache 基金会	CNNVD-202203-499	Hazelcast

	Delta	CNNVD-202203-2491	代码问题漏洞（CNNVD-202203-175）
	Hazelcast	CNNVD-202203-175	
	Pascom	CNNVD-202203-1794	
	Signiant	CNNVD-202203-921	
	Spatie	CNNVD-202203-1506	
	Tensent	CNNVD-202203-898	
		CNNVD-202203-899	
	VMware	CNNVD-202203-2058	
	Veeam	CNNVD-202203-1596	
	WordPress 基金会	CNNVD-202203-1918	
		CNNVD-202203-2066	
	Zenario	CNNVD-202203-1340	
	个人开发者	CNNVD-202203-084	
		CNNVD-202203-086	
		CNNVD-202203-471	
		CNNVD-202203-639	
		CNNVD-202203-640	
		CNNVD-202203-1463	
		CNNVD-202203-1470	
		CNNVD-202203-1578	
		CNNVD-202203-1795	
		CNNVD-202203-1799	
		CNNVD-202203-1881	
		CNNVD-202203-1956	
		CNNVD-202203-2044	
		CNNVD-202203-2233	
授权问题	Apple	CNNVD-202203-1298	Fortinet FortiMail 授权问题漏洞（CNNVD-202203-024）
	Cacti 团队	CNNVD-202203-185	
	Fortinet	CNNVD-202203-024	
	MingSoft	CNNVD-202203-491	
	OpenVPN	CNNVD-202203-1823	
	Schneider Electric	CNNVD-202203-810	
		CNNVD-202203-811	
	Sophos	CNNVD-202203-2229	
	个人开发者	CNNVD-202203-916	
		CNNVD-202203-1169	
		CNNVD-202203-1524	
		CNNVD-202203-1980	
操作系统命令注入	ARRIS	CNNVD-202203-1495	SonicWall SSLVPN 操作系统命令注入漏洞（CNNVD-202203-1558）
		CNNVD-202203-1497	
		CNNVD-202203-1498	
		CNNVD-202203-1499	
		CNNVD-202203-1501	

		CNNVD-202203-1502	
		CNNVD-202203-1505	
		CNNVD-202203-1509	
	Asciidoctor 组织	CNNVD-202203-2711	
	NEC	CNNVD-202203-982	
	Red Hat	CNNVD-202203-2113	
	SonicWall	CNNVD-202203-1558	
	Tenda	CNNVD-202203-2081	
		CNNVD-202203-2082	
		CNNVD-202203-2084	
		CNNVD-202203-2085	
		CNNVD-202203-2086	
		CNNVD-202203-2088	
		CNNVD-202203-2091	
		CNNVD-202203-2092	
		CNNVD-202203-2102	
		CNNVD-202203-2106	
		CNNVD-202203-2107	
	VMware	CNNVD-202203-2059	
	Zyxel	CNNVD-202203-015	
	个人开发者	CNNVD-202203-014	
		CNNVD-202203-039	
		CNNVD-202203-134	
		CNNVD-202203-467	
		CNNVD-202203-512	
		CNNVD-202203-914	
		CNNVD-202203-1585	
缓冲区错误	Apache 基金会	CNNVD-202203-1270	Apache HTTP Server 缓冲区错误漏洞（CNNVD-202203-1270）
	Apple	CNNVD-202203-1267	
	FromSoftware	CNNVD-202203-1874	
	Google	CNNVD-202203-556	
	HP	CNNVD-202203-2055	
	Huawei	CNNVD-202203-986	
	Palo Alto Networks	CNNVD-202203-999	
	Schneider Electric	CNNVD-202203-812	
	Siemens	CNNVD-202203-657	
	SonicWall	CNNVD-202203-2271	
	Synology	CNNVD-202203-2220	
	Tenda	CNNVD-202203-461	
		CNNVD-202203-462	
		CNNVD-202203-890	
		CNNVD-202203-1830	
		CNNVD-202203-1831	

		CNNVD-202203-1832	
		CNNVD-202203-1833	
		CNNVD-202203-1834	
		CNNVD-202203-1835	
		CNNVD-202203-1836	
		CNNVD-202203-1837	
		CNNVD-202203-1838	
		CNNVD-202203-1839	
		CNNVD-202203-1840	
		CNNVD-202203-1841	
		CNNVD-202203-1842	
		CNNVD-202203-1843	
		CNNVD-202203-1844	
		CNNVD-202203-1845	
		CNNVD-202203-1846	
		CNNVD-202203-2042	
	Tianocore 社区	CNNVD-202203-178	
		CNNVD-202203-180	
	个人开发者	CNNVD-202203-513	
		CNNVD-202203-864	
		CNNVD-202203-1200	
		CNNVD-202203-1529	
		CNNVD-202203-2010	
访问控制错误	PTC	CNNVD-202203-745	Siemens Mendix 访问控制错误漏洞（CNNVD-202203-743）
		CNNVD-202203-758	
	Siemens	CNNVD-202203-743	
	Transportation Systems Sector	CNNVD-202203-497	
	WAVLINK	CNNVD-202203-1573	
	个人开发者	CNNVD-202203-2130	
资源管理错误	Apple	CNNVD-202203-1256	General Electric Renewable Energy MDS Radios 资源管理错误漏洞（CNNVD-202203-2652）
	General Electric	CNNVD-202203-2652	
	个人开发者	CNNVD-202203-2299	
输入验证错误	Apache 基金会	CNNVD-202203-1299	Genian NAC 输入验证错误漏洞（CNNVD-202203-2254）
	Apple	CNNVD-202203-1263	
	Bitrix	CNNVD-202203-2000	
	Fortinet	CNNVD-202203-031	
	Genians	CNNVD-202203-2254	
	Puppet 实验室	CNNVD-202203-092	
	SAP	CNNVD-202203-797	
	Siemens	CNNVD-202203-660	

	个人开发者	CNNVD-202203-151	
		CNNVD-202203-514	
		CNNVD-202203-967	
		CNNVD-202203-1461	

1. Rapid7 Nexpose SQL 注入漏洞（CNNVD-202203-1606）

Rapid7 Nexpose 是美国 Rapid7 公司的一套能够利用扫描结果深度探测网络的漏洞管理软件。该软件支持扫描配置环境的错误、漏洞、恶意软件等。

Rapid7 Nexpose 6.6.93 版本及之前版本 存在安全漏洞，该漏洞源于 Rapid7 Nexpose 6.6.93 版本及之前版本易受 SQL 注入。该漏洞允许攻击者操纵 SearchCriteria 中的“ANY”和“OR”运算符，并注入 SQL 代码。Rapid7 Nexpose 6.6.129 版本修复了此问题。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://docs.rapid7.com/release-notes/nexpose/20220302/

2. Hazelcast 代码问题漏洞（CNNVD-202203-175）

Hazelcast（Hazelcast IMDG）是美国 Hazelcast 公司的一套可扩展的开源数据分发平台。该平台支持多种分布式数据结构，支持分布式缓存等功能。

Hazelcast 5.1 之前版本的 XML 存在安全漏洞，该漏洞源于 GitHub 存储库 Hazelcast 5.1 之前版本的 XML 外部实体引用限制不当。

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/hazelcast/hazelcast/commit/4d6b666cd0291abd618c3b95cdbb51aa4208e748

3. Fortinet FortiMail 授权问题漏洞（CNNVD-202203-024）

Fortinet FortiMail 是美国飞塔（Fortinet）公司的一套电子邮件安全网关产品。该产品提供电子邮件安全防护和数据保护等功能。

FortiMail 7.0.1 之前存在授权问题漏洞，该漏洞源于远程攻击者可利用该漏洞通过观察某个系统的属性来有效地猜测某个管理帐户的身份验证令牌。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://fortiguard.com/psirt/FG-IR-21-099

4. SonicWall SSLVPN 操作系统命令注入漏洞（CNNVD-202203-1558）

SonicWall SSLVPN是美国SonicWall公司的一个适用于 Windows 和 Linux 用户的透明软件应用程序。使远程用户能够安全地连接到公司网络。

SonicWall SSLVPN 存在安全漏洞，以下产品和版本受到影响：SRA系列 9.0.0.5-19sv 及更早版本,SMA100 系列 9.0.0.9-26sv 及更早版本。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2022-0001

5. Apache HTTP Server 缓冲区错误漏洞（CNNVD-202203-1270）

Apache HTTP Server 是美国阿帕奇（Apache）基金会的一款开源网页服务器。该服务器具有快速、可靠且可通过简单的 API 进行扩充的特点。

Apache HTTP Server 2.4 版本 2.4.52 和之前版本的 mod_sed 中存在缓冲区错误漏洞，该漏洞允许攻击者使用攻击者提供的数据覆盖堆内存。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://httpd.apache.org/security/vulnerabilities_24.html

6. Siemens Mendix 访问控制错误漏洞（CNNVD-202203-743）

Siemens Mendix 是德国西门子（Siemens）公司的一套低代码应用程序开发平台。该平台提供应用程序开发、测试、部署和迭代等功能。

Mendix Forgot Password Appstore module 存在安全漏洞，该漏洞源于在 Mendix Forgot Password Appstore 模块(所有版本>= V3.3.0 < V3.5.1)的某些配置中，威胁参与者可以使用注册流劫持任意用户帐户。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://cert-portal.siemens.com/productcert/pdf/ssa-134279.pdf

7. General Electric Renewable Energy MDS Radios 资源管理错误漏洞（CNNVD-202203-2652）

General Electric Renewable Energy MDS Radios 是美国 General Electric 公司的一系列工业无线解决方案。

General Electric Renewable Energy MDS iNET/iNET II/SD/TD220/TD220MAX Radios 存在资源管理错误漏洞。攻击者使用身份验证代码可以使无线电重置为出厂默认配置并重新启动。

目前厂商已发布升级补丁以修复漏洞，详情请关注厂商主页：https://www.gegridsolutions.com/communications/wireless.htm

8. Genian NAC 输入验证错误漏洞（CNNVD-202203-2254）

Genians Genian NAC 是韩国 Genians 公司的一款网络安全和访问控制软件。可帮助企业识别启用 IP 的设备、管理漏洞并检查设备配置以保护网络访问环境。

Genian NAC V5.0 Genian NAC Suite V5.0 Genian NAC Suite V4.0 存在安全漏洞，该漏洞源于软件中文件名参数验证不足。攻击者可以利用该漏洞在 NAC 中的所有连接节点上执行具有 SYSTEM 权限的任意恶意代码。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://genians.co.kr/products/genian-nac/?gclid=EAIaIQobChMI5qvMmPPE9gIVoZvCCh3rMANmEAAYASAAEgJuCvD_BwE

1.4.2 高危漏洞实例

2022 年 3 月高危漏洞共 710 个，其中重要漏洞实例如表 6 所示。

表 6　2022 年 3 月高危漏洞实例

漏洞类型	厂商	CNNVD 编号	漏洞实例

SQL 注入	Artica	CNNVD-202203-938	Fortinet FortiWLM SQL 注入漏洞（CNNVD-202203-035）
	Fortinet	CNNVD-202203-035	
	OS4Ed	CNNVD-202203-133	
		CNNVD-202203-135	
	Siemens	CNNVD-202203-757	
	Slims 社区	CNNVD-202203-1569	
		CNNVD-202203-1581	
		CNNVD-202203-1582	
	Softinventive Lab	CNNVD-202203-889	
	Sophos	CNNVD-202203-1952	
	WordPress 基金会	CNNVD-202203-600	
		CNNVD-202203-605	
		CNNVD-202203-607	
		CNNVD-202203-613	
		CNNVD-202203-626	
		CNNVD-202203-634	
		CNNVD-202203-635	
		CNNVD-202203-1322	
		CNNVD-202203-1349	
		CNNVD-202203-1362	
		CNNVD-202203-1812	
		CNNVD-202203-1973	
	YesWiki 组织	CNNVD-202203-2231	
	个人开发者	CNNVD-202203-018	
		CNNVD-202203-025	
		CNNVD-202203-109	
		CNNVD-202203-911	
		CNNVD-202203-1467	
		CNNVD-202203-1533	
		CNNVD-202203-1863	
		CNNVD-202203-1895	
		CNNVD-202203-2129	
		CNNVD-202203-2223	
		CNNVD-202203-2440	
	北京智慧远景科技产业有限公司	CNNVD-202203-1875	
代码问题	Admidio 团队	CNNVD-202203-1872	Rapid7 Insight Agent 代码问题漏洞（CNNVD-202203-1605）
	Alibaba	CNNVD-202203-2033	
	Anaconda	CNNVD-202203-1589	
	Big Ant Studios	CNNVD-202203-1947	
	Ethereum 社区	CNNVD-202203-454	
	GOGS 团队	CNNVD-202203-1889	
	KINGSOFT	CNNVD-202203-1535	

		CNNVD-202203-1536	
		CNNVD-202203-1537	
	Ligeo Archives	CNNVD-202203-1601	
	PTC	CNNVD-202203-759	
	Python 基金会	CNNVD-202203-523	
	Quicklert	CNNVD-202203-959	
	Rapid7	CNNVD-202203-1605	
	Razer	CNNVD-202203-2095	
	Red Hat	CNNVD-202203-1963	
	Siemens	CNNVD-202203-656	
		CNNVD-202203-756	
	SmarterTools	CNNVD-202203-1286	
	Softing	CNNVD-202203-1207	
	SuiteCRM 团队	CNNVD-202203-919	
	Sylius	CNNVD-202203-1380	
	Trend Micro	CNNVD-202203-592	
	Veeam	CNNVD-202203-1591	
	WordPress 基金会	CNNVD-202203-599	
		CNNVD-202203-637	
		CNNVD-202203-1819	
		CNNVD-202203-1913	
	Wordline	CNNVD-202203-139	
	Yokogawa	CNNVD-202203-1153	
	个人开发者	CNNVD-202203-108	
		CNNVD-202203-136	
		CNNVD-202203-842	
		CNNVD-202203-848	
		CNNVD-202203-1294	
		CNNVD-202203-1519	
		CNNVD-202203-1544	
		CNNVD-202203-1813	
		CNNVD-202203-1865	
		CNNVD-202203-1883	
		CNNVD-202203-1884	
		CNNVD-202203-1953	
		CNNVD-202203-1976	
		CNNVD-202203-2030	
		CNNVD-202203-2373	
		CNNVD-202203-2606	
		CNNVD-202203-2607	
	中国赞赞网络科技公司	CNNVD-202203-1886	
授权问题	Acer	CNNVD-202203-912	Zyxel USG/ZyWALL 授权问题漏洞
		CNNVD-202203-913	

	Apache 基金会	CNNVD-202203-2031	（CNNVD-202203-2311）
	Apple	CNNVD-202203-1271	
	EFM	CNNVD-202203-2257	
	Gitea 社区	CNNVD-202203-843	
	LG	CNNVD-202203-464	
	Luna	CNNVD-202203-1212	
	Microweber 社区	CNNVD-202203-012	
	Netgear	CNNVD-202203-2053	
		CNNVD-202203-2060	
	Shopware	CNNVD-202203-834	
	TP-Link	CNNVD-202203-958	
	Veeam	CNNVD-202203-1595	
	Webmin 社区	CNNVD-202203-075	
	Yokogawa	CNNVD-202203-1152	
	Zyxel	CNNVD-202203-2311	
	otris	CNNVD-202203-970	
	个人开发者	CNNVD-202203-646	
		CNNVD-202203-1391	
		CNNVD-202203-2138	
		CNNVD-202203-2246	
操作系统命令注入	Fortinet	CNNVD-202203-036	Fortinet FortiWLM 操作系统命令注入漏洞（CNNVD-202203-036）
		CNNVD-202203-045	
	Netgear	CNNVD-202203-2286	
		CNNVD-202203-2287	
		CNNVD-202203-2288	
	Stripe	CNNVD-202203-833	
	TP-Link	CNNVD-202203-493	
	Yokogawa	CNNVD-202203-1160	
缓冲区错误	Accusoft	CNNVD-202203-2705	Linux kernel 缓冲区错误漏洞（CNNVD-202203-2027）
	Adobe	CNNVD-202203-792	
		CNNVD-202203-793	
		CNNVD-202203-795	
		CNNVD-202203-796	
		CNNVD-202203-798	
		CNNVD-202203-1815	
		CNNVD-202203-1817	
	AppNeta	CNNVD-202203-2281	
		CNNVD-202203-2282	
		CNNVD-202203-2283	
	Apple	CNNVD-202203-1237	
		CNNVD-202203-1240	
		CNNVD-202203-1248	
		CNNVD-202203-1251	

		CNNVD-202203-1254	
		CNNVD-202203-1255	
		CNNVD-202203-1257	
		CNNVD-202203-1262	
		CNNVD-202203-1264	
		CNNVD-202203-1275	
		CNNVD-202203-1285	
		CNNVD-202203-1293	
		CNNVD-202203-1295	
		CNNVD-202203-1297	
		CNNVD-202203-1300	
		CNNVD-202203-1301	
		CNNVD-202203-1302	
		CNNVD-202203-1307	
		CNNVD-202203-1308	
		CNNVD-202203-1311	
		CNNVD-202203-1313	
		CNNVD-202203-1315	
		CNNVD-202203-1317	
		CNNVD-202203-1319	
		CNNVD-202203-1324	
		CNNVD-202203-1330	
		CNNVD-202203-2671	
	EOSIO 社区	CNNVD-202203-1551	
	Fuji Electric	CNNVD-202203-2665	
		CNNVD-202203-2666	
		CNNVD-202203-2669	
	Google	CNNVD-202203-062	
		CNNVD-202203-524	
		CNNVD-202203-525	
		CNNVD-202203-526	
		CNNVD-202203-535	
		CNNVD-202203-541	
	HP	CNNVD-202203-2056	
	Huawei	CNNVD-202203-971	
		CNNVD-202203-975	
		CNNVD-202203-977	
		CNNVD-202203-978	
	IBM	CNNVD-202203-1365	
	KINGSOFT	CNNVD-202203-1538	
	Linux 基金会	CNNVD-202203-1869	
		CNNVD-202203-2027	
	Mattermost	CNNVD-202203-933	

	Microsoft	CNNVD-202203-732	
		CNNVD-202203-733	
		CNNVD-202203-734	
		CNNVD-202203-738	
		CNNVD-202203-764	
	MikroTik	CNNVD-202203-1534	
	Mozilla 基金会	CNNVD-202203-709	
	Netgear	CNNVD-202203-1801	
	Omron	CNNVD-202203-650	
		CNNVD-202203-651	
		CNNVD-202203-2480	
		CNNVD-202203-2484	
	Samsung	CNNVD-202203-861	
	Siemens	CNNVD-202203-746	
	Silicon Graphics	CNNVD-202203-787	
	Tenda	CNNVD-202203-867	
		CNNVD-202203-870	
		CNNVD-202203-871	
		CNNVD-202203-872	
		CNNVD-202203-873	
		CNNVD-202203-874	
		CNNVD-202203-875	
		CNNVD-202203-876	
		CNNVD-202203-877	
		CNNVD-202203-878	
		CNNVD-202203-879	
		CNNVD-202203-880	
		CNNVD-202203-881	
		CNNVD-202203-882	
		CNNVD-202203-883	
		CNNVD-202203-884	
		CNNVD-202203-942	
		CNNVD-202203-2038	
		CNNVD-202203-2039	
	Webroot	CNNVD-202203-1496	
		CNNVD-202203-1503	
	Yandex	CNNVD-202203-1383	
		CNNVD-202203-1386	
		CNNVD-202203-1387	
		CNNVD-202203-1389	
	digikey	CNNVD-202203-654	
	个人开发者	CNNVD-202203-120	
		CNNVD-202203-126	

		CNNVD-202203-141	
		CNNVD-202203-143	
		CNNVD-202203-145	
		CNNVD-202203-146	
		CNNVD-202203-147	
		CNNVD-202203-500	
		CNNVD-202203-502	
		CNNVD-202203-1165	
		CNNVD-202203-1222	
		CNNVD-202203-1360	
		CNNVD-202203-1375	
		CNNVD-202203-1381	
		CNNVD-202203-1559	
		CNNVD-202203-1560	
		CNNVD-202203-1562	
		CNNVD-202203-1961	
		CNNVD-202203-2040	
		CNNVD-202203-2045	
		CNNVD-202203-2046	
		CNNVD-202203-2116	
		CNNVD-202203-2221	
访问控制错误	Apple	CNNVD-202203-1335	Cisco Ultra Cloud Core 访问控制错误漏洞（CNNVD-202203-104）
	Cisco	CNNVD-202203-104	
	IBM	CNNVD-202203-1870	
	Mcafee	CNNVD-202203-1032	
	Netgear	CNNVD-202203-1571	
	PTC	CNNVD-202203-754	
	Phicomm	CNNVD-202203-803	
		CNNVD-202203-807	
	Siemens	CNNVD-202203-749	
	WAVLINK	CNNVD-202203-1572	
	WordPress 基金会	CNNVD-202203-617	
		CNNVD-202203-1928	
	openEuler 社区	CNNVD-202203-1195	
	个人开发者	CNNVD-202203-008	
		CNNVD-202203-1908	
资源管理错误	Apple	CNNVD-202203-1235	Cisco Identity Services Engine 资源管理错误漏洞（CNNVD-202203-103）
		CNNVD-202203-1241	
		CNNVD-202203-1259	
		CNNVD-202203-1276	
		CNNVD-202203-1281	
		CNNVD-202203-1289	
	Cisco	CNNVD-202203-103	

	Ethereum 社区	CNNVD-202203-453	
	FreeTAKTeam 团队	CNNVD-202203-1037	
	Google	CNNVD-202203-064	
		CNNVD-202203-066	
		CNNVD-202203-067	
		CNNVD-202203-070	
		CNNVD-202203-071	
		CNNVD-202203-506	
		CNNVD-202203-551	
		CNNVD-202203-559	
		CNNVD-202203-1429	
		CNNVD-202203-1439	
		CNNVD-202203-1443	
		CNNVD-202203-1445	
		CNNVD-202203-1446	
		CNNVD-202203-1447	
		CNNVD-202203-1448	
		CNNVD-202203-1449	
		CNNVD-202203-2448	
		CNNVD-202203-2460	
		CNNVD-202203-2462	
		CNNVD-202203-2467	
	IBM	CNNVD-202203-450	
	Linux 基金会	CNNVD-202203-1821	
	Mozilla 基金会	CNNVD-202203-501	
		CNNVD-202203-503	
		CNNVD-202203-704	
		CNNVD-202203-705	
	Omron	CNNVD-202203-652	
		CNNVD-202203-653	
		CNNVD-202203-2481	
	PDFTron	CNNVD-202203-891	
	Qualcomm	CNNVD-202203-611	
	Yokogawa	CNNVD-202203-1154	
	个人开发者	CNNVD-202203-774	
		CNNVD-202203-836	
		CNNVD-202203-990	
		CNNVD-202203-2021	
		CNNVD-202203-2279	
		CNNVD-202203-2537	
输入验证错误	Apache 基金会	CNNVD-202203-1274	SolarWinds Web Help Desk 输入验证错误漏洞
		CNNVD-202203-2032	
	Apple	CNNVD-202203-1244	

		CNNVD-202203-1273	（CNNVD-202203-2252）
	Autodesk	CNNVD-202203-590	
		CNNVD-202203-596	
	Dell	CNNVD-202203-1202	
		CNNVD-202203-1203	
		CNNVD-202203-1204	
		CNNVD-202203-1205	
		CNNVD-202203-1206	
	Google	CNNVD-202203-534	
		CNNVD-202203-589	
		CNNVD-202203-2458	
	LEAD Technologies	CNNVD-202203-1483	
	Linux 基金会	CNNVD-202203-1504	
	Microsoft	CNNVD-202203-701	
	Microweber 社区	CNNVD-202203-1151	
		CNNVD-202203-1984	
	NVIDIA	CNNVD-202203-2359	
	Nozomi Networks	CNNVD-202203-2122	
		CNNVD-202203-2123	
	PowerDNS	CNNVD-202203-2225	
	SolarWinds	CNNVD-202203-2252	
	WordPress 基金会	CNNVD-202203-1333	
	个人开发者	CNNVD-202203-1430	
		CNNVD-202203-1903	

1. Fortinet FortiWLM SQL 注入漏洞（CNNVD-202203-035）

Fortinet FortiWLM 是美国飞塔（Fortinet）公司的一个无线管理器。

Fortinet FortiWLM 存在 SQL 注入漏洞，该漏洞允许攻击者利用该漏洞通过向 AP 监视器处理程序发送精心设计的 HTTP 请求来执行未经授权的代码或命令。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://fortiguard.com/advisory/FG-IR-21-189

2. Rapid7 Insight Agent 代码问题漏洞（CNNVD-202203-1605）

Rapid7 Insight Agent 是美国 Rapid7 公司的一款轻量级软件。该软件能够从 IT 资产中收集数据。

Rapid7 Insight Agent 3.1.2.38 版本及之前版本 存在安全漏洞，该漏洞源于 Rapid7 Insight Agent 3.1.2.38 版本及之前版本在使用 runas.exe 时没有正确双引号。该漏洞允许攻击者提升权限和对计算机的持久访问。Rapid7 Insight Agent 3.1.3.80 版本修复了此问题。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://docs.rapid7.com/release-notes/insightagent/20220225/

3. Zyxel USG/ZyWALL 授权问题漏洞（CNNVD-202203-2311）

Zyxel USG/ZyWALL 是中国合勤科技（Zyxel）公司的一款防火墙。

Zyxel USG/ZyWALL 4.20 版本至 4.70 版本、USG FLEX 4.50 版本至 5.20 版本、ATP 4.32 版本至 5.20 版本、VPN 4.30 版本至 5.20 版本、NSG 1.20 版本至 1.33 Patch 4 版本存在安全漏洞，攻击者利用该漏洞绕过 Web 身份验证并获得设备的管理访问权限。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://www.zyxel.com/support/Zyxel-security-advisory-for-authentication-bypass-vulnerability-of-firewalls.shtml

4. Fortinet FortiWLM 操作系统命令注入漏洞（CNNVD-202203-036）

Fortinet FortiWLM 是美国飞塔（Fortinet）公司的一个无线管理器。

Fortinet FortiWLM 存在操作系统命令注入漏洞，该漏洞允许攻击者利用该漏洞通过精心制作的 HTTP 请求执行未经授权的代码或命令。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://fortiguard.com/advisory/FG-IR-21-128

5. Linux kernel 缓冲区错误漏洞（CNNVD-202203-2027）

Linux kernel 是美国 Linux 基金会的开源操作系统 Linux 所使用的内核。

Linux kernel 5.16.15 之前版本存在安全漏洞，该漏洞源于 net/ipv4/esp4.c 和 net/ipv6/esp6.c 中 IPsec ESP 代码存在缓冲区溢出。本地攻击者可利用该漏洞通过覆盖内核堆对象获得特权。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.16.15

6. Cisco Ultra Cloud Core 访问控制错误漏洞（CNNVD-202203-104）

Cisco Ultra Cloud Core 是美国思科（Cisco）公司的一种基于 Kubernetes 的解决方案。可为 Cisco 基于容器的 5G 应用程序提供通用执行环境。

Cisco Ultra Cloud Core 存在访问控制错误漏洞，该漏洞允许经过身份验证的本地攻击者可利用该漏洞升级受影响设备上的权限。此漏洞是由于受影响的 CLI 中没有足够的访问控制。攻击者利用该漏洞可以通过一个 CEE ConfD CLI 用户进行身份验证并执行特定的 CLI 命令来利用这个漏洞。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-uccsmi-prvesc-BQHGe4cm

7. Cisco Identity Services Engine 资源管理错误漏洞（CNNVD-202203-103）

Cisco Identity Services Engine（ISE）是美国思科（Cisco）公司的一款环境感知平台（ISE 身份服务引擎）。该平台通过收集网络、用户和设备中的实时信息，制定并实施相应策略来监管网络。

Cisco Identity Services Engine 存在资源管理错误漏洞，该漏洞源于某些 RADIUS 请求处理不当。未经认证的远程攻击者可利用该漏洞导致受影响的系统停止处理 RADIUS 报文。

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-ise-dos-JLh9TxBp

8. SolarWinds Web Help Desk 输入验证错误漏洞（CNNVD-202203-2252）

Solarwinds Web Help Desk 是美国 Solarwinds 公司的一套服务台和资产管理软件。该软件支持集中式知识库、IT 资产管理、项目和任务管理等功能。

SolarWinds Web Help Desk 12.7.8 及其之前版本存在安全漏洞，该漏洞源于应用缺少有效的输入验证与过滤。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://www.solarwinds.com/trust-center/security-advisories/CVE-2021-35254

二、漏洞平台推送情况

2022 年 3 月漏洞平台推送漏洞 6112 个。

表 7　2022 年 3 月漏洞平台推送情况表

序号	漏洞平台	漏洞总量
1	漏洞盒子	4264
2	补天平台	1848
推送总计		6112

三、接报漏洞情况

2022 年 2 月接报漏洞 1471 个，其中信息技术产品漏洞（通用型漏洞）573 个，网络信息系统漏洞（事件型漏洞）898 个。

表 8　2022 年 3 月接报漏洞情况表

序号	报送单位	漏洞数量
1	西安四叶草信息技术有限公司	226
2	南京众智维信息科技有限公司	111
3	北京华云安信息技术有限公司	102
4	道普信息技术有限公司	101
5	北京山石网科信息技术有限公司	83
6	长春嘉诚信息技术股份有限公司	68
7	杭州默安科技有限公司	50

8	北京天融信网络安全技术有限公司	46
9	中电信数智科技有限公司	39
10	山东新潮信息技术有限公司	36
11	南京禾盾信息科技有限公司	30
12	北京安华金和科技有限公司	30
13	上海斗象信息科技有限公司	28
14	广州竞远安全技术股份有限公司	25
15	个人	24
16	杭州安恒信息技术股份有限公司	22
17	北京安全共识科技有限公司	21
18	广州锦行网络科技有限公司	20
19	星云博创科技有限公司	20
20	安徽长泰科技有限公司	20
21	成都忆享科技有限公司	20
22	北京数字观星科技有限公司	19
23	北京奇虎科技有限公司	17
24	北京华胜久安科技有限公司	15
25	新华三技术有限公司	15
26	北京世纪先承信息安全科技有限公司	15
27	杭州迪普科技股份有限公司	13
28	恒安嘉新（北京）科技股份公司	13
29	北京水木羽林科技有限公司	13
30	北京中金安服科技有限公司	13
31	杭州立思辰安科科技有限公司	10
32	北京国舜科技股份有限公司	8
33	天津市兴先道科技有限公司	8
34	上海谋乐网络科技有限公司	8
35	华为技术有限公司	7
36	百度公司	7
37	杭州孝道科技有限公司	7
38	中兴通讯股份有限公司	7
39	深圳市深信服电子科技有限公司	6
40	北京时代新威信息技术有限公司	6
41	深圳海云安网络安全技术有限公司	6
42	上海安识网络科技有限公司	6
43	浪潮电子信息产业股份有限公司	6
44	中国—东盟信息港股份有限公司	6
45	上海上讯信息技术股份有限公司	6
46	重庆梦之想科技有限责任公司	6
47	成都尺物科技有限公司	5
48	中国电信集团系统集成有限责任公司	5
49	北京安天网络安全技术有限公司	5
50	北京威努特技术有限公司	5

51	厦门服云信息科技有限公司	5
52	北京江南天安科技有限公司	5
53	烽台科技（北京）有限公司	5
54	西安交大捷普网络科技有限公司	4
55	上海安洵信息技术有限公司	4
56	北京优炫软件股份有限公司	4
57	北京机沃科技有限公司	4
58	金诺碳投环保科技（北京）有限公司	4
59	湖南省金盾信息安全等级保护评估中心有限公司	4
60	天翼数智科技（ 北京）有限公司	4
61	三六零数字安全科技集团有限公司	3
62	北京安信天行科技有限公司	3
63	战略支援部队信息工程大学	3
64	北京智游网安科技有限公司	3
65	北京世纪百易网络有限公司	3
66	北京神州绿盟科技有限公司	3
67	浙江大学，贵州大学	2
68	赛尔网络有限公司山东分公司	2
69	山西轩辕信息安全技术有限公司	2
70	北京华顺信安科技有限公司	2
71	腾讯科技（北京）有限公司	2
72	北京永信至诚科技股份有限公司	2
73	墨菲未来科技(北京)有限公司	1
74	广州易东信息安全技术有限公司	1
75	北京安帝科技有限公司	1
76	深圳开源互联网安全技术有限公司	1
77	江苏中新赛克工业互联网安全技术创新中心有限公司	1
78	河南听潮盛世信息技术有限公司	1
79	广西电网有限责任公司信息中心	1
80	博智安全科技股份有限公司	1
81	北京六方云信息技术有限公司	1
82	海南神州希望网络有限公司	1
83	新疆安疆科技有限公司	1
84	马上消费金融	1
85	湖南省金盾信息安全等级保护评估中心	1
报送合计		1471

四、重大漏洞通报

4.1 Linux kernel 安全漏洞的通报

近日，国家信息安全漏洞库（CNNVD）收到关于Linux kernel安全漏洞（CNNVD-202203-522、CVE-2022-0847）情况的报送。成功利用此漏洞的攻击者，可提升本地用户权限。Linux Kernel 5.8-5.16.11、5.8-5.15.25、5.8-5.10.102 等版本均受此漏洞影响。目前，Linux 官方已发布新版本修复了漏洞，请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

Linux kernel是美国Linux基金会发布的开源操作系统Linux所使用的内核。Linux kernel存在安全漏洞，攻击者可利用漏洞覆盖重写任意可读文件中的数据，从而将普通权限的用户提升到root权限用户。

. 危害影响

成功利用此漏洞的攻击者，可在默认配置下提升本地用户权限。Linux Kernel 5.8-5.16.11、5.8-5.15.25、5.8-5.10.102 等版本均受此漏洞影响。

. 修复建议

目前，Linux官方已发布新版本修复了漏洞，请用户及时确认是否受到漏洞影响，尽快采取修补措施。官方链接如下：

https://www.debian.org/security/2022/dsa-5092

4.2 Redis 代码注入漏洞的通报

近日，国家信息安全漏洞库（CNNVD）收到关于Redis代码注入漏洞（CNNVD-202202-1622、CVE-2022-0543）情况的报送。成功利用此漏洞的攻击者，可在目标服务器远程执行恶意代码,进而控制目标服务器。Redis 5.x系列 5.0.14 以下版本、Redis 6.x系列 6.0.16 以下版本、Redis 7.x系列 7.0-rc2 以下版本均受漏洞影响。目前，Redis官方已发布新版本修复了漏洞，请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

Redis是美国Redis Labs公司的一套开源的使用ANSI C编写、支持网络、可基于内存亦可持久化的日志型、键值（Key-Value）存储数据库。Redis存在代码注入漏洞,攻击者可利用该漏洞在未授权的情况下，构造恶意数据执行沙箱逃逸攻击，最终获取服务器最高权限。

. 危害影响

成功利用此漏洞的攻击者，可在目标服务器远程执行恶意代码,进而控制目标服务器。Redis 5.x系列 5.0.14 以下版本、Redis 6.x系列 6.0.16 以下版本、Redis 7.x系列 7.0-rc2 以下版本均受漏洞影响。

. 修复建议

目前，Redis官方已发布新版本修复了漏洞，请用户及时确认是否受到漏洞影响，尽快采取修补措施。官方链接如下：

https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=1005787