国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2023 年 11 月 13 日-2023 年 11 月 19 日 **2023 年第 46 期**

本周漏洞态势研判情况

本周信息安全漏洞威胁整体评价级别为**中**。

国家信息安全漏洞共享平台（以下简称 CNVD）本周共收集、整理信息安全漏洞 375 个，其中高危漏洞 140 个、中危漏洞 212 个、低危漏洞 23 个。漏洞平均分值为 6.27。本周收录的漏洞中，涉及 0day 漏洞 301 个（占 80%），其中互联网上出现“GetSimple CMS 跨站脚本漏洞、livehelperchat 跨站脚本漏洞（CNVD-2023-86325）”等零日代码攻击漏洞。本周 CNVD 接到的涉及党政机关和企事业单位的漏洞总数 41601 个，与上周（23920 个）环比增多 74%。

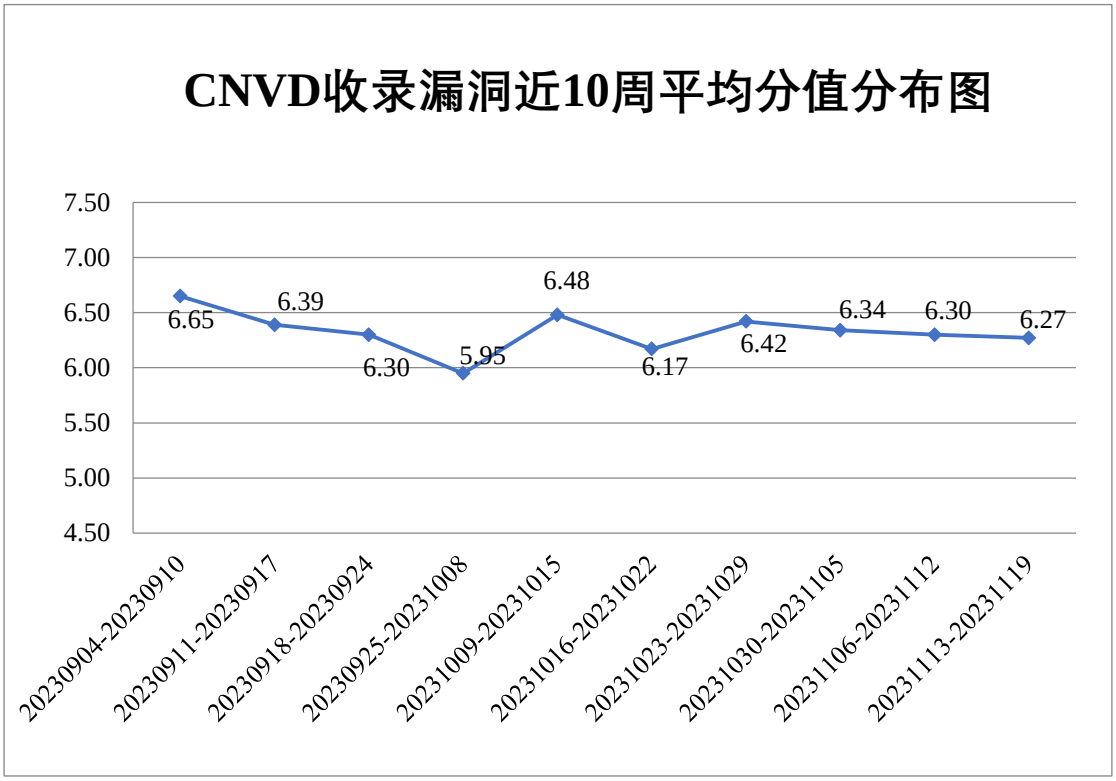

图 1 CNVD 收录漏洞近 10 周平均分值分布图

本周漏洞事件处置情况

本周，CNVD 向银行、保险、能源等重要行业单位通报漏洞事件 16 起，向基础电信企业通报漏洞事件 14 起，协调 CNCERT 各分中心验证和处置涉及地方重要部门漏洞事件 1077 起，协调教育行业应急组织验证和处置高校科研院所系统漏洞事件 257 起，向国家上级信息安全协调机构上报涉及部委门户、子站或直属单位信息系统漏洞事件 57 起。

此外，CNVD 通过已建立的联系机制或涉事单位公开联系渠道向以下单位通报了其信息系统或软硬件产品存在的漏洞，具体处置单位情况如下所示：

卓豪（中国）技术有限公司、珠海金山办公软件有限公司、重庆晓羊智教信息技术有限公司、众勤通信设备贸易（上海）有限公司、中煤科工集团信息技术有限公司、郑州卡卡罗特软件科技有限公司、正方软件股份有限公司、真珍斑马技术贸易（上海）有限公司、长沙市同迅计算机科技有限公司、长春吉大正元信息技术股份有限公司、友讯电子设备（上海）有限公司、用友网络科技股份有限公司、新天科技股份有限公司、新疆易投在线信息科技有限公司、携程科技（上海）有限公司、夏普科技（上海）有限公司、西安交大捷普网络科技有限公司、西安大西信息科技有限公司、武汉升望科技有限公司、武汉三佳医疗信息技术有限公司、无锡赛博盈科科技有限公司、威博通科技（上海）有限公司、万洲电气股份有限公司、统信软件技术有限公司、天维尔信息科技股份有限公司、天津神舟通用数据技术有限公司、唐山飞泽科技有限公司、太原易思软件技术有限公司、台州市黄岩猎英人力资源有限公司、松立控股集团股份有限公司、世邦通信股份有限公司、石家庄市征红网络科技有限公司、施耐德电气（中国）有限公司、深圳智慧光迅信息技术有限公司、深圳市中启教育科技有限公司、深圳市新微云科技有限公司、深圳市唯传科技有限公司、深圳市蓝凌软件股份有限公司、深圳市科漫达智能管理科技有限公司、深圳市捷顺科技实业股份有限公司、深圳市吉祥腾达科技有限公司、深圳市惠尔顿信息技术有限公司、深圳市海伦司品牌管理有限公司、深圳锐取信息技术股份有限公司、深圳科士达科技股份有限公司、深信服科技股份有限公司、上海宜采软件科技有限公司、上海茸易科技有限公司、上海普华科技发展股份有限公司、上海穆云智能科技有限公司、上海明厦物联网科技有限公司、上海华测导航技术股份有限公司、上海亘岩网络科技有限公司、上海泛微网络科技股份有限公司、上海创旗天下科技股份有限公司、上海博达数据通信有限公司、上海百胜软件股份有限公司、陕西小伙伴网络科技有限公司、山西复盛公药业集团有限公司医药分公司、山东中维世纪科技股份有限公司、山东山大华天软件有限公司、厦门攸信信息技术有限公司、赛昂斯（深圳）智能科技有限公司、任子行网络技术股份有限公司、青岛智链顺达科技有限公司、奇偶信息科技（上海）有限公司、普元信息技术股份有限公司、普联技术有限公司、南京横渡医疗技术有限公司、联想集团、理光（中国）投资有限公司、浪潮电子信息产业股份有限公司、朗坤智慧科技股份有限公司、蓝卓数字科技有限公司、科华数据股份有限公司、

京瓷办公信息系统（中国）有限公司、江苏麦维智能科技有限公司、江苏开沃汽车有限公司、江苏百拓信息技术有限公司、佳能（中国）有限公司、吉翁电子（深圳）有限公司、吉首市微商互联信息技术有限公司、惠普贸易（上海）有限公司、华信永道（北京）科技股份有限公司、湖南亿美科技有限公司、杭州中宝科技有限公司、杭州雄伟科技开发股份有限公司、杭州启汇科技有限公司、杭州海康威视数字技术股份有限公司、杭州飞致云信息科技有限公司、哈尔滨伟成科技有限公司、广州图创计算机软件开发有限公司、广州赛意信息科技股份有限公司、广州璐华信息技术有限公司、广联达科技股份有限公司、广东星之源信息科技有限公司、广东飞企互联科技股份有限公司、富士施乐（中国）有限公司、福建传爱网络科技有限公司、烽火通信科技股份有限公司、东软教育科技集团有限公司、鼎点视讯科技有限公司、帝国软件、大麦科技发展有限公司、成都生动网络科技有限公司、畅捷通信息技术股份有限公司、沧州市凡诺广告传媒有限公司、北京卓软在线信息技术有限公司、北京中科华博科技有限公司、北京中犇科技有限公司、北京智慧远景科技产业有限公司、北京致远互联软件股份有限公司、北京亿赛通科技发展有限责任公司、北京星网锐捷网络技术有限公司、北京万户网络技术有限公司、北京通达信科科技有限公司、北京上元信安技术有限公司、北京如易行科技有限公司、北京米尔伟业科技有限公司、北京联达动力信息科技发展有限公司、北京朗新天霁软件技术有限公司、北京凯特伟业科技有限公司、北京金和网络股份有限公司、北京火绒网络科技有限公司、北京宏景世纪软件股份有限公司、北京汉王智远科技有限公司、北京果心科技有限公司、北京格尺科技有限公司、北京北信源软件股份有限公司、北京佰才邦技术股份有限公司、北京百卓网络技术有限公司、北京安博通科技股份有限公司、安美世纪（北京）科技有限公司、爱普生（中国）有限公司和 ZZCMS。

本周，CNVD 发布了《Microsoft 发布 2023 年 11 月安全更新》。详情参见 CNVD 网站公告内容。

https://www.cnvd.org.cn/webinfo/show/9466

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，天津市国瑞数码安全系统股份有限公司、北京天融信网络安全技术有限公司、新华三技术有限公司、北京启明星辰信息安全技术有限公司、北京神州绿盟科技有限公司等单位报送公开收集的漏洞数量较多。亚信科技（成都）有限公司、江苏金盾检测技术股份有限公司、中孚安全技术有限公司、安徽锋刃信息科技有限公司、联想集团、快页信息技术有限公司、北京山石网科信息技术有限公司、杭州默安科技有限公司、河南东方云盾信息技术有限公司、河南灵创电子科技有限公司、北京远禾科技有限公司、赛尔网络有限公司、统信软件技术有限公司、内蒙古洞明科技有限公司、北京微步在线科技有限公司、国网山东省电力公司、河南悦海数安科技有限

公司、任子行网络技术股份有限公司、安徽天行网安信息安全技术有限公司、成方金融科技有限公司上海分公司、江苏君立华域信息安全技术股份有限公司、合肥梆梆信息科技有限公司、山石网科通信技术股份有限公司、广东粤密技术服务有限公司、杭州美创科技有限公司、江苏晟晖信息科技有限公司、中电福富信息科技有限公司、江苏极元信息技术有限公司、济南三泽信息安全测评有限公司、四川中成基业安全技术有限公司、山东新潮信息技术有限公司、平安银河实验室、广州安亿信软件科技有限公司、成都天天网安信息安全技术有限公司、成都安美勤信息技术股份有限公司、武汉非尼克斯软件技术有限公司、宁夏凯信特信息科技有限公司、星云博创科技有限公司、贵州多彩网安科技有限公司、中国邮政储蓄银行股份有限公司、山东云天安全技术有限公司、上海直画科技有限公司、异图（上海）科技有限责任公司、内蒙古中叶信息技术有限责任公司、超聚变数字技术有限公司、北京君云天下科技有限公司、北京时代新威信息技术有限公司及其他个人白帽子向 CNVD 提交了 41601 个以事件型漏洞为主的原创漏洞，其中包括奇安信网神（补天平台）、斗象科技（漏洞盒子）、三六零数字安全科技集团有限公司和上海交大向 CNVD 共享的白帽子报送的 38537 条原创漏洞信息。

表 1 漏洞报送情况统计表

报送单位或个人	漏洞报送数量	原创漏洞数
奇安信网神（补天平台）	21833	21833
斗象科技（漏洞盒子）	15902	15902
天津市国瑞数码安全系统股份有限公司	3123	0
北京天融信网络安全技术有限公司	1049	46
新华三技术有限公司	609	0
北京启明星辰信息安全技术有限公司	441	38
三六零数字安全科技集团有限公司	423	423
北京神州绿盟科技有限公司	398	218
上海交大	379	379
北京数字观星科技有限公司	254	0
深信服科技股份有限公司	194	0

阿里云计算有限公司	180	22
安天科技集团股份有限公司	60	0
北京知道创宇信息技术有限公司	58	8
京东科技信息技术有限公司	50	32
远江盛邦（北京）网络安全科技股份有限公司	31	31
杭州迪普科技股份有限公司	19	0
北京升鑫网络科技有限公司（青藤云）	15	15
北京长亭科技有限公司	13	0
中电科网络安全科技股份有限公司	8	8
南京联成科技发展股份有限公司	6	6
中国电信股份有限公司网络安全产品运营中心	3	3
北京信联数安科技有限公司	2	2
西安四叶草信息技术有限公司	2	2
亚信科技（成都）有限公司	650	650
江苏金盾检测技术股份有限公司	103	103
西门子（中国）有限公司	52	0
中孚安全技术有限公司	40	40

安徽锋刃信息科技有限公司	34	34
联想集团	18	18
快页信息技术有限公司	14	14
北京山石网科信息技术有限公司	11	11
杭州默安科技有限公司	10	10
河南东方云盾信息技术有限公司	9	9
河南灵创电子科技有限公司	6	6
北京远禾科技有限公司	5	5
赛尔网络有限公司	5	5
统信软件技术有限公司	5	5
内蒙古洞明科技有限公司	4	4
北京微步在线科技有限公司	4	4
国网山东省电力公司	4	4
河南悦海数安科技有限公司	4	4
任子行网络技术股份有限公司	3	3
安徽天行网安信息安全技术有限公司	3	3
成方金融科技有限公司上海分公司	2	2
江苏君立华域信息安全技术股份有限公司	2	2
合肥梆梆信息科技有限公司	2	2

山石网科通信技术股份有限公司	2	2
广东粤密技术服务有限公司	2	2
杭州美创科技有限公司	2	2
江苏晟晖信息科技有限公司	1	1
中电福富信息科技有限公司	1	1
江苏极元信息技术有限公司	1	1
济南三泽信息安全测评有限公司	1	1
四川中成基业安全技术有限公司	1	1
山东新潮信息技术有限公司	1	1
平安银河实验室	1	1
广州安亿信软件科技有限公司	1	1
成都天天网安信息安全技术有限公司	1	1
成都安美勤信息技术股份有限公司	1	1
武汉非尼克斯软件技术有限公司	1	1
宁夏凯信特信息科技有限公司	1	1
星云博创科技有限公司	1	1
贵州多彩网安科技有限公司	1	1
中国邮政储蓄银行股份有限公司	1	1

山东云天安全技术有限公司	1	1
上海直画科技有限公司	1	1
异图（上海）科技有限责任公司	1	1
内蒙古中叶信息技术有限责任公司	1	1
超聚变数字技术有限公司	1	1
北京君云天下科技有限公司	1	1
北京时代新威信息技术有限公司	1	1
CNCERT 广西分中心	3	3
CNCERT 贵州分中心	3	3
CNCERT 河北分中心	2	2
个人	1659	1659
报送总计	47737	41601

本周漏洞按类型和厂商统计

本周，CNVD 收录了 375 个漏洞。WEB 应用 171 个，应用程序 121 个，网络设备（交换机、路由器等网络端设备）57 个，安全产品 15 个，智能设备（物联网终端设备）6 个，操作系统 3 个，数据库 2 个。

表 2 漏洞按影响类型统计表

漏洞影响对象类型	漏洞数量
WEB 应用	171
应用程序	121
网络设备（交换机、路由器等网络端设备）	57
安全产品	15
智能设备（物联网终端设备）	6
操作系统	3
数据库	2

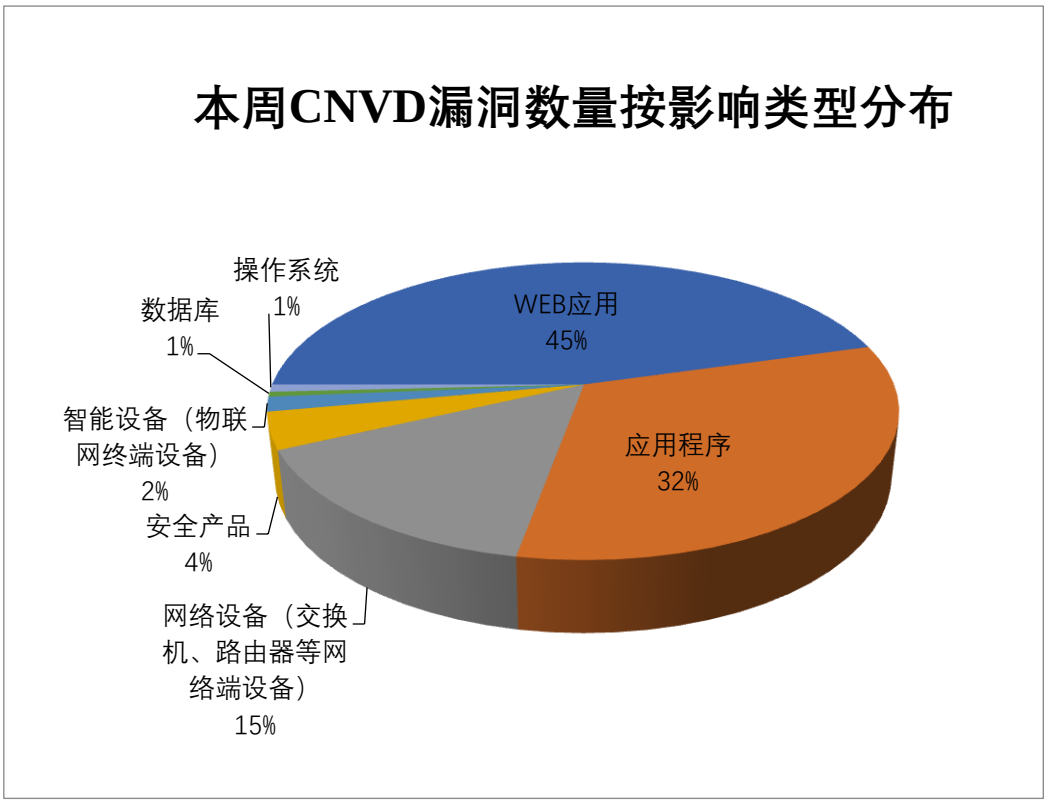

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Siemens、Microsoft、用友网络科技股份有限公司等多家厂商的产品，部分漏洞数量按厂商统计如表 3 所示。

表 3 漏洞产品涉及厂商分布统计表

序号	厂商（产品）	漏洞数量	所占比例
1	Siemens	18	5%
2	Microsoft	15	4%
3	用友网络科技股份有限公司	14	4%
4	北京星网锐捷网络技术有限公司	13	3%
5	Apache	11	3%
6	Oracle	10	3%
7	Cisco	9	2%
8	北京百卓网络技术有限公司	8	2%
9	WordPress	6	2%
10	其他	271	72%

本周行业漏洞收录情况

本周，CNVD 收录了 38 个电信行业漏洞，55 个移动互联网行业漏洞，15 个工控行

业漏洞（如下图所示）。其中，“多款 Siemens 产品输入验证错误漏洞（CNVD-2023-86591）、Cisco Small Business Series Switches 堆缓冲区溢出漏洞、Siemens OPC UA Modeling Editor (SiOME) XML 外部实体注入漏洞”等漏洞的综合评级为“高危”。相关厂商已经发布了漏洞的修补程序，请参照 CNVD 相关行业漏洞库链接。

电信行业漏洞链接：http://telecom.cnvd.org.cn/

移动互联网行业漏洞链接：http://mi.cnvd.org.cn/

工控系统行业漏洞链接：http://ics.cnvd.org.cn/

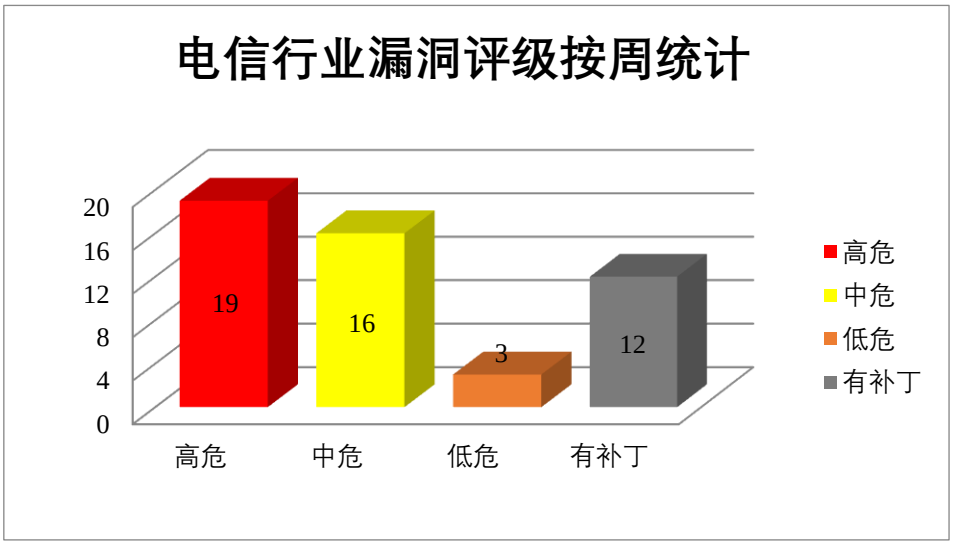

图 3 电信行业漏洞统计

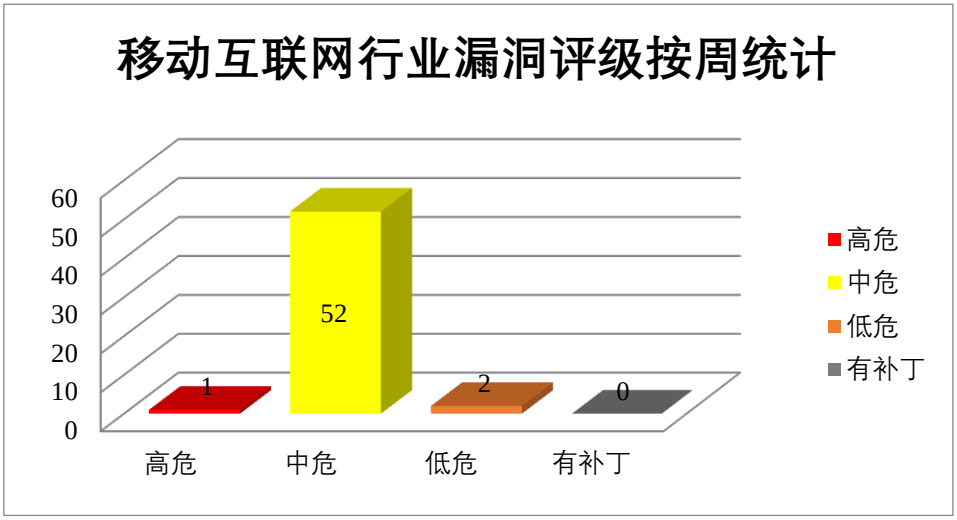

图 4 移动互联网行业漏洞统计

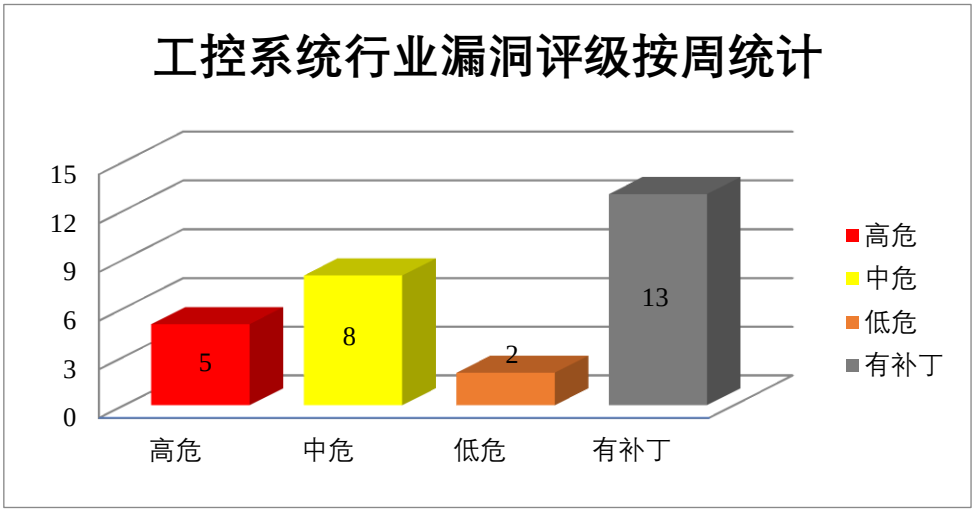

图 5 工控系统行业漏洞统计

本周重要漏洞安全告警

本周，CNVD 整理和发布以下重要安全漏洞信息。

1、Microsoft 产品安全漏洞

Microsoft Dynamics 365 是美国微软（Microsoft）公司的一套适用于跨国企业的 ERP 业务解决方案。该产品包括财务管理、生产管理和商业智能管理等。Microsoft Office Visio 是美国微软（Microsoft）公司的 Office 软件系列中的负责绘制流程图和示意图的软件。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞获取敏感信息，在系统上执行任意代码。

CNVD 收录的相关漏洞包括：Microsoft Dynamics 365 (On-Premises)信息泄露漏洞（CNVD-2023-85889）、Microsoft Office Visio 远程代码执行漏洞（CNVD-2023-85900、CNVD-2023-85901、CNVD-2023-85902、CNVD-2023-85904、CNVD-2023-85905、CNVD-2023-85906）、Microsoft Office Visio 信息泄露漏洞。其中，除“Microsoft Dynamics 365 (On-Premises)信息泄露漏洞（CNVD-2023-85889）”外，其余漏洞的综合评级为“高危”。目前，厂商已经发布了上述漏洞的修补程序。CNVD 提醒用户及时下载补丁更新，避免引发漏洞相关的网络安全事件。

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2023-85889

https://www.cnvd.org.cn/flaw/show/CNVD-2023-85900

https://www.cnvd.org.cn/flaw/show/CNVD-2023-85901

https://www.cnvd.org.cn/flaw/show/CNVD-2023-85902

https://www.cnvd.org.cn/flaw/show/CNVD-2023-85903

https://www.cnvd.org.cn/flaw/show/CNVD-2023-85904

https://www.cnvd.org.cn/flaw/show/CNVD-2023-85905

https://www.cnvd.org.cn/flaw/show/CNVD-2023-85906

2、Cisco 产品安全漏洞

Cisco Firepower Management Center（FMC）是美国思科（Cisco）公司的新一代防火墙管理中心软件。Cisco Secure Network Analytics (Stealthwatch) 是支持跨平台的网络流数据收集的解决方案。Cisco Small Business Series Switches 是美国思科（Cisco）公司的交换机产品。Cisco IOS XE Software 是美国思科（Cisco）公司的一个操作系统。用于企业有线和无线访问，汇聚，核心和 WAN 的单一操作系统，Cisco IOS XE 降低了业务和网络的复杂性。Cisco Firepower Management Center（FMC）是美国思科（Cisco）公司的新一代防火墙管理中心软件。Cisco Nexus Dashboard 是美国思科（Cisco）公司的一个单一控制台。能够简化数据中心网络的运营和管理。Cisco Finesse 是美国思科（Cisco）公司的一套呼叫中心管理软件。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞在受影响的设备上执行代码，造成拒绝服务。

CNVD 收录的相关漏洞包括：Cisco Firepower Management Center 跨站脚本漏洞（CNVD-2023-85951、CNVD-2023-85950、CNVD-2023-85952）、Cisco Secure Network Analytics 远程代码执行漏洞（CNVD-2023-85955）、Cisco Small Business Series Switches 堆缓冲区溢出漏洞、Cisco IOS XE 存在命令注入漏洞、Cisco Nexus Dashboard 拒绝服务漏洞、Cisco Finesse 拒绝服务漏洞。其中，除“Cisco Firepower Management Center 跨站脚本漏洞（CNVD-2023-85951、CNVD-2023-85950、CNVD-2023-85952）”外，其余的综合评级为“高危”。目前，厂商已经发布了上述漏洞的修补程序。CNVD 提醒用户及时下载补丁更新，避免引发漏洞相关的网络安全事件。

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2023-85951

https://www.cnvd.org.cn/flaw/show/CNVD-2023-85950

https://www.cnvd.org.cn/flaw/show/CNVD-2023-85955

https://www.cnvd.org.cn/flaw/show/CNVD-2023-85954

https://www.cnvd.org.cn/flaw/show/CNVD-2023-85953

https://www.cnvd.org.cn/flaw/show/CNVD-2023-85952

https://www.cnvd.org.cn/flaw/show/CNVD-2023-85957

https://www.cnvd.org.cn/flaw/show/CNVD-2023-85956

3、Apache 产品安全漏洞

Apache Airflow 是美国阿帕奇（Apache）基金会的一套用于创建、管理和监控工作流程的开源平台。该平台具有可扩展和动态监控等特点。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞获取敏感信息，在系统上执行任意代码，导致系统拒绝服务等。

CNVD 收录的相关漏洞包括：Apache Airflow 信息泄露漏洞（CNVD-2023-85609、CNVD-2023-85611、CNVD-2023-85610、CNVD-2023-85612、CNVD-2023-85617）、A

pache Airflow 代码执行漏洞（CNVD-2023-85614、CNVD-2023-85613）、Apache Airflow 代码问题漏洞（CNVD-2023-85615）。其中，“Apache Airflow 代码执行漏洞（CNVD-2023-85614、CNVD-2023-85613）、Apache Airflow 代码问题漏洞（CNVD-2023-85615）、Apache Airflow 信息泄露漏洞（CNVD-2023-85617）”漏洞的综合评级为“高危”。目前，厂商已经发布了上述漏洞的修补程序。CNVD 提醒用户及时下载补丁更新，避免引发漏洞相关的网络安全事件。

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2023-85609
https://www.cnvd.org.cn/flaw/show/CNVD-2023-85611
https://www.cnvd.org.cn/flaw/show/CNVD-2023-85610
https://www.cnvd.org.cn/flaw/show/CNVD-2023-85614
https://www.cnvd.org.cn/flaw/show/CNVD-2023-85613
https://www.cnvd.org.cn/flaw/show/CNVD-2023-85612
https://www.cnvd.org.cn/flaw/show/CNVD-2023-85615
https://www.cnvd.org.cn/flaw/show/CNVD-2023-85617

4、 Siemens 产品安全漏洞

SIMATIC PCS neo 是一种分布式控制系统（DCS）。COMOS 是一个用于协同工厂设计、运营和管理的统一数据平台，支持在整个工厂生命周期内收集、处理、保存和分发信息。Mendix 是一个高生产力的应用程序平台，能够大规模构建和持续改进移动和 web 应用程序。SCALANCE M-800、MUM-800 和 S615 以及 RUGGEDCOM RM1224 是工业路由器。SCALANCE W 产品是用于连接工业组件的无线通信设备，如可编程逻辑控制器（PLC）或人机界面（HMI），符合 IEEE 802.11 标准（802.11ac、802.11a/b/g/h 和/或 802.11n）。SCALANCE W-1700 产品是基于 IEEE 802.11ac 标准的无线通信设备。它们用于连接各种 WLAN 设备（接入点或客户端，取决于操作模式），重点关注工业组件，如可编程逻辑控制器（PLC）或人机界面（HMI）等。SCALANCE X 交换机用于连接可编程逻辑控制器（PLC）或人机界面（HMI）等工业组件。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞在基础数据库中执行 SQL 语句，提升权限，执行任意代码或造成拒绝服务等。

CNVD 收录的相关漏洞包括：Siemens SIMATIC PCS neo 跨站脚本漏洞、Siemens COMOS 访问控制错误漏洞（CNVD-2023-86339）、Siemens SIMATIC PCS neo 身份验证错误漏洞、Siemens SIMATIC PCS neo SQL 注入漏洞、Siemens Mendix 认证绕过漏洞、Siemens COMOS 缓冲区溢出漏洞（CNVD-2023-86341）、Siemens COMOS 访问控制错误漏洞、多款 Siemens 产品输入验证错误漏洞（CNVD-2023-86591）。其中，“Siemens COMOS 访问控制错误漏洞（CNVD-2023-86339）、Siemens COMOS 缓冲区溢出漏洞（CNVD-2023-86341）、Siemens COMOS 访问控制错误漏洞、多款 Siemens 产品输入验证错误漏洞（CNVD-2023-86591）”漏洞的综合评级为“高危”。目前，

厂商已经发布了上述漏洞的修补程序。CNVD 提醒用户及时下载补丁更新，避免引发漏洞相关的网络安全事件。

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2023-86335
https://www.cnvd.org.cn/flaw/show/CNVD-2023-86339
https://www.cnvd.org.cn/flaw/show/CNVD-2023-86338
https://www.cnvd.org.cn/flaw/show/CNVD-2023-86337
https://www.cnvd.org.cn/flaw/show/CNVD-2023-86343
https://www.cnvd.org.cn/flaw/show/CNVD-2023-86341
https://www.cnvd.org.cn/flaw/show/CNVD-2023-86340
https://www.cnvd.org.cn/flaw/show/CNVD-2023-86591

5、IceCMS 跨站请求伪造漏洞

IceCMS 是一个基于 Spring Boot + Vue 前后端分离的内容管理系统。本周，IceCMS 被披露存在跨站请求伪造漏洞。攻击者可利用该漏洞伪造恶意请求诱骗受害者点击执行敏感操作。目前，厂商尚未发布上述漏洞的修补程序。CNVD 提醒广大用户随时关注厂商主页，以获取最新版本。参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2023-86329

更多高危漏洞如表 4 所示，详细信息可根据 CNVD 编号，在 CNVD 官网进行查询。参考链接：http://www.cnvd.org.cn/flaw/list

表 4 部分重要高危漏洞列表

CNVD 编号	漏洞名称	综合评级	修复方式
CNVD-2023-85608	Apache Airflow 日志信息泄露漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/apache/airflow/pull/34954
CNVD-2023-85615	Apache Airflow 代码问题漏洞（CNVD-2023-85615）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://lists.apache.org/thread/g5c9vcn27lr14go48thrjpo6f4vw571r
CNVD-2023-85901	Microsoft Office Visio 远程代码执行漏洞（CNVD-2023-85901）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36865
CNVD-2023-85954	Cisco Small Business Series Switches 堆缓冲区溢出漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv

CNVD-2023-86340	Siemens COMOS 访问控制错误漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://cert-portal.siemens.com/productcert/html/ssa-137900.html
CNVD-2023-85613	Apache Airflow 代码执行漏洞（CNVD-2023-85613）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://lists.apache.org/thread/ggthr5pn42bn6wcr25hxnykjzh4ntw7z
CNVD-2023-85903	Microsoft Office Visio 信息泄露漏洞	高	目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载：https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-21741
CNVD-2023-85956	Cisco Finesse 拒绝服务漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-finesse-proxy-dos-vY5dQhrV
CNVD-2023-86588	Siemens OPC UA Modeling Editor (SiOME) XML 外部实体注入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://cert-portal.siemens.com/productcert/html/ssa-197270.html
CNVD-2023-85905	Microsoft Office Visio 远程代码执行漏洞（CNVD-2023-85905）	高	目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载：https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-21737

小结：本周，Microsoft 产品被披露存在多个漏洞，攻击者可利用漏洞获取敏感信息，在系统上执行任意代码。此外，Cisco、Apache、Siemens 等多款产品被披露存在多个漏洞，攻击者可利用漏洞在基础数据库中执行 SQL 语句，获取敏感信息，提升权限，执行任意代码或造成拒绝服务等。另外，IceCMS 被披露存在跨站请求伪造漏洞。攻击者可利用该漏洞伪造恶意请求诱骗受害者点击执行敏感操作。建议相关用户随时关注上述厂商主页，及时获取修复补丁或解决方案。

本周重要漏洞攻击验证情况

本周，CNVD 建议注意防范以下已公开漏洞攻击验证情况。

1、GetSimpleCMS 跨站脚本漏洞

验证描述

GetSimpleCMS 是个人开发者的一个内容管理系统。

GetSimpleCMS v3.4.0a 版本存在跨站脚本漏洞，该漏洞源于应用对用户提供的数据缺乏有效过滤与转义，远程攻击者可利用该漏洞通过 Components.php 函数使用精心设计的有效负载执行任意代码。

验证信息

POC 链接：https://github.com/Num-Nine/CVE/wiki/GetSimplecms-exists-to-store-xss

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2023-86327

信息提供者

新华三技术有限公司

注：以上验证信息(方法)可能带有攻击性，仅供安全研究之用。请广大用户加强对漏洞的防范工作，尽快下载相关补丁。

本周漏洞要闻速递

1. Intel 披露 Reptar 安全漏洞，可绕过 CPU 安全边界

近日，Intel 修复了其现代台式机、服务器、移动和嵌入式 CPU（包括最新的 Alder Lake、Raptor Lake 和 Sapphire Rapids 微体系结构）中的一个 CPU 漏洞。攻击者可以利用 CVE-2023-23583 漏洞提升权限、访问敏感信息或触发拒绝服务状态。

参考链接：https://www.freebuf.com/news/383884.html

2. Fortinet 警告 FortiSIEM 中存在命令注入漏洞

Fortinet 提醒注意 FortiSIEM 报表服务器中存在一个系统命令注入漏洞，未经身份验证的远程攻击者可利用该漏洞通过特制的 API 请求执行命令。

参考链接：https://www.bleepingcomputer.com/news/security/fortinet-warns-of-critical-command-injection-bug-in-fortisiem/

关于 CNVD

国家信息安全漏洞共享平台（China National Vulnerability Database，简称 CNVD）是由 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的国家网络安全漏洞库，致力于建立国家统一的信息安全漏洞收集、发布、验证、分析等应急处理体系。

关于 CNCERT

国家计算机网络应急技术处理协调中心（简称“国家互联网应急中心”，英文简称是 CNCERT 或 CNCERT/CC），成立于 2002 年 9 月，为非政府非盈利的网络安全技术中心，是我国计算机网络应急处理体系中的牵头单位。

作为国家级应急中心，CNCERT 的主要职责是：按照“积极预防、及时发现、快速响应、力保恢复”的方针，开展互联网网络安全事件的预防、发现、预警和协调处置等工作，维护国家公共互联网安全，保障基础信息网络和重要信息系统的安全运行。

网址：www.cert.org.cn

邮箱：vreport@cert.org.cn

电话：010-82991537