国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2018 年 8 月 6 日-2018 年 8 月 12 日 **2018 年第 32 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 213 个，其中高危漏洞 66 个、中危漏洞 144 个、低危漏洞 3 个。漏洞平均分值为 6.27。本周收录的漏洞中，涉及 0day 漏洞 63 个（占 30%），其中互联网上出现“Ericsson-LG iPECS NMS 30M 目录遍历漏洞、Adobe Reader PDF 本地请求注入漏洞”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事件型漏洞总数 893 个，与上周（534 个）环比增长 67%。

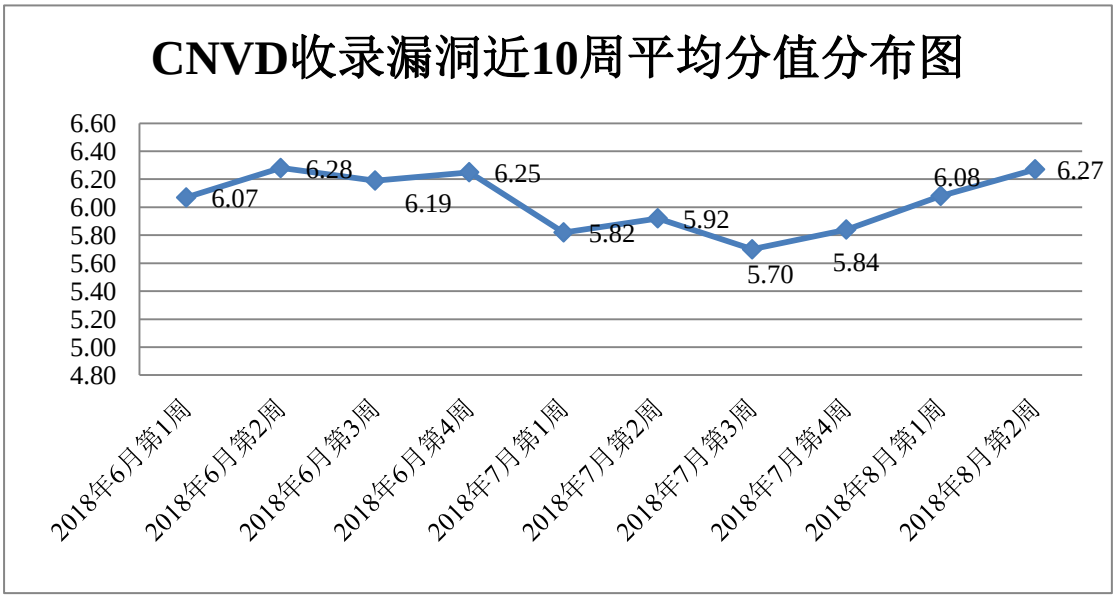

图 1 CNVD 收录漏洞近 10 周平均分值分布图

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，北京天融信网络安全技术有限公司、哈尔滨安天科技股份有限公司、新华三技术有限公司、华为技术有限公司、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。山东云天安全技术有限公司、南京联成科技发展股份有限公司、中新网络信息安全股份有限公司、任子行网络技术股份有限公司、河南信安世纪科技有限公司、上海银基信息安全技术股份有限公司、新疆海狼科技有限公司、山石网科通信技术有限公司、河北网信智安信息技术有限公司、江苏省信息安全测评中心、福建六壬网安股份有限公司、上海纽盾科技股份有限公司及其他个人白帽子向 CNVD 提交了 893 个以事件型漏洞为主的原创漏洞，其中包括 360 网神（补天平台）和漏洞盒子向 CNVD 共享的白帽子报送的 582 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	原创漏洞数量
北京天融信网络安全技术有限公司	309	8
漏洞盒子	295	295
360 网神（补天平台）	287	287
哈尔滨安天科技股份有限公司	200	0
新华三技术有限公司	120	0
华为技术有限公司	117	0
北京神州绿盟科技有限公司	98	0
北京数字观星科技有限公司	73	0
中国电信集团系统集成有限责任公司	62	0
北京无声信息技术有限公司	48	40
恒安嘉新(北京)科技股份公司	30	0
深圳市深信服电子科技有限公司	15	4
厦门服云信息科技有限公司	10	0
北京知道创宇信息技术有限公司	5	3
深圳市深信服电子科技有限公司	4	4
沈阳东软系统集成工程有限公司	2	2

西安四叶草信息技术有限公司	1	1
山东云天安全技术有限公司	53	53
南京联成科技发展股份有限公司	16	16
中新网络信息安全股份有限公司	15	15
任子行网络技术股份有限公司	9	9
河南信安世纪科技有限公司	4	4
上海银基信息安全技术股份有限公司	4	4
新疆海狼科技有限公司	3	3
山石网科通信技术有限公司	2	2
河北网信智安信息技术有限公司	1	1
江苏省信息安全测评中心	1	1
福建六壬网安股份有限公司	1	1
上海纽盾科技股份有限公司	1	1
CNCERT 吉林分中心	4	4
CNCERT 河北分中心	3	3
CNCERT 新疆分中心	3	3
CNCERT 天津分中心	2	2
CNCERT 甘肃分中心	2	2
CNCERT 贵州分中心	1	1
个人	124	124
报送总计	1925	893

本周漏洞按类型和厂商统计

本周，CNVD 收录了 213 个漏洞。应用程序漏洞 166 个，网络设备漏洞 19 个，WEB 应用漏洞 17 个，操作系统漏洞 10 个，数据库漏洞 1 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
应用程序漏洞	166
网络设备漏洞	19
WEB 应用漏洞	17
操作系统漏洞	10
数据库漏洞	1

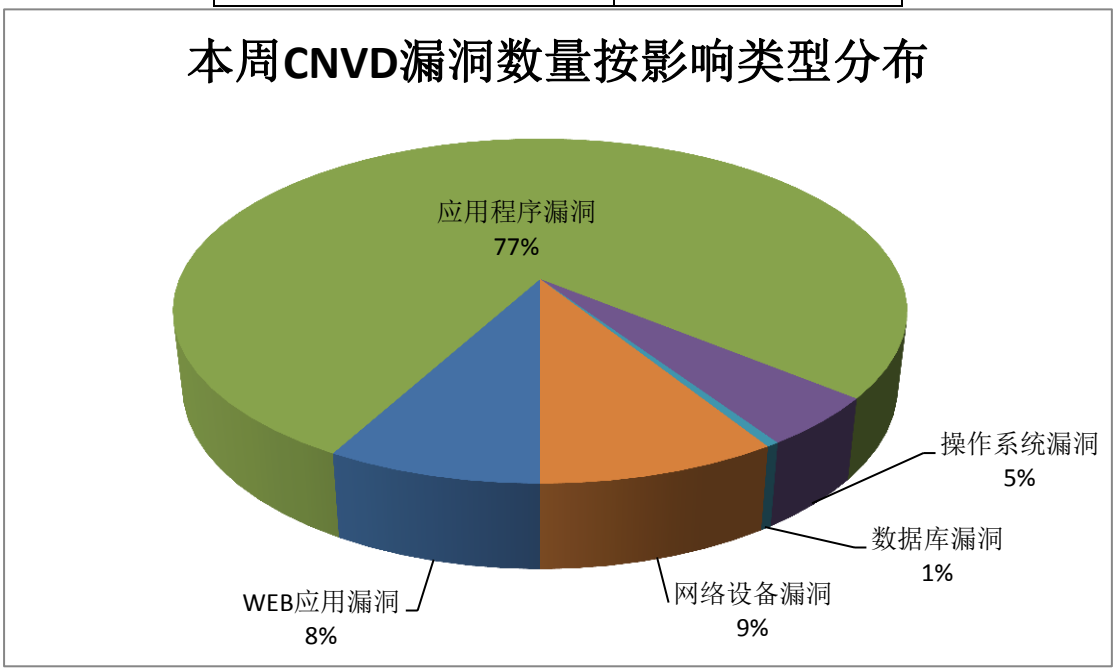

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Foxit、Adobe、Apple 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	Foxit	34	16%
2	Adobe	28	13%
3	Apple	14	6%
4	Mozilla	13	6%
5	INSTEON	10	5%
6	CloudBees	8	4%
7	Apache	6	3%
8	Libtiff	6	3%

9	SAP	6	3%
10	其他	88	41%

本周行业漏洞收录情况

本周，CNVD 收录了 2 个电信行业漏洞，11 个移动互联网行业漏洞（如下图所示）。其中，“Apple iOS Wi-Fi 内存破坏漏洞、Apple iOS 任意代码执行漏洞（CNVD-2018-14963）”的综合评级为“高危”。相关厂商已经发布了上述漏洞的修补程序，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/

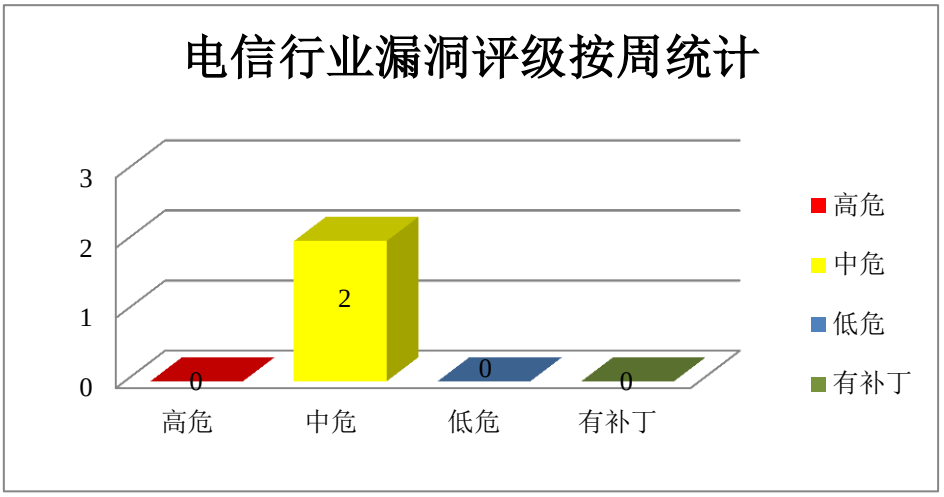

图 3 电信行业漏洞统计

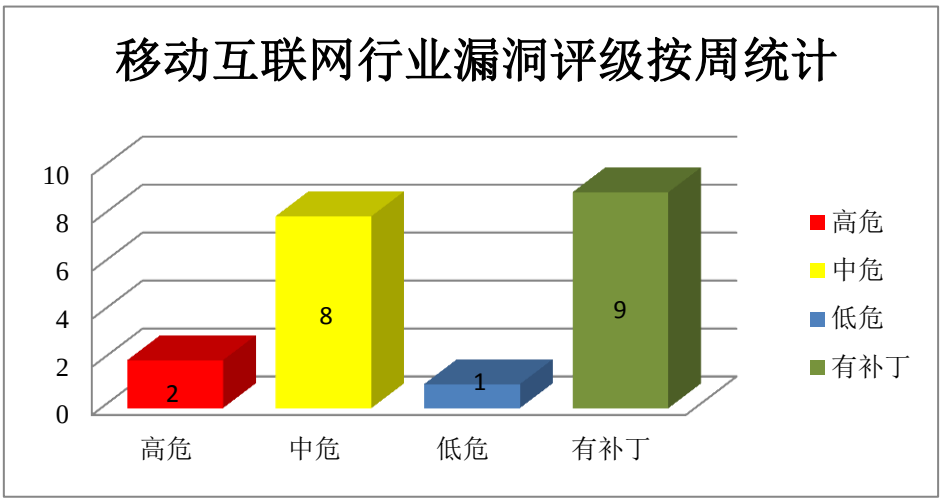

图 4 移动互联网行业漏洞统计

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、Foxit 产品安全漏洞

Foxit Reader（旧名：Foxit PDF Reader）是一套用来阅读 PDF 格式文件的软件。Foxit Reader 是一套自由使用的软件，操作系统主要以 Microsoft Windows 为主，且只要有 Win32 执行环境的操作系统上皆可使用。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞执行任意代码。

CNVD 收录的相关漏洞包括：Foxit Reader 类型混淆远程代码执行漏洞（CNVD-2018-15068、CNVD-2018-15067、CNVD-2018-15070、CNVD-2018-15069、CNVD-2018-15071）、Foxit Reader 任意文件写入远程代码执行漏洞（CNVD-2018-15093）、Foxit PDF Reader JavaScript 引擎内存错误引用漏洞（CNVD-2018-15095、CNVD-2018-15096）。其中，“Foxit Reader 任意文件写入远程代码执行漏洞（CNVD-2018-15093）、Foxit PDF Reader JavaScript 引擎内存错误引用漏洞（CNVD-2018-15095、CNVD-2018-15096）”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：http://www.cnvd.org.cn/flaw/show/CNVD-2018-15068
http://www.cnvd.org.cn/flaw/show/CNVD-2018-15067
http://www.cnvd.org.cn/flaw/show/CNVD-2018-15070
http://www.cnvd.org.cn/flaw/show/CNVD-2018-15069
http://www.cnvd.org.cn/flaw/show/CNVD-2018-15071
http://www.cnvd.org.cn/flaw/show/CNVD-2018-15093
http://www.cnvd.org.cn/flaw/show/CNVD-2018-15095
http://www.cnvd.org.cn/flaw/show/CNVD-2018-15096

2、Adobe 产品安全漏洞

Adobe Acrobat 是一款 PDF 编辑软件。Adobe Reader(也被称为 Acrobat Reader)是一款 PDF 文件阅读软件。本周，上述产品被披露存在越界写入漏洞，攻击者可利用漏洞执行任意代码。

CNVD 收录的相关漏洞包括：Adobe Acrobat 和 Reader 越界写入漏洞（CNVD-2018-14926、CNVD-2018-14927、CNVD-2018-14928、CNVD-2018-14929、CNVD-2018-14932、CNVD-2018-14930、CNVD-2018-14931、CNVD-2018-14933）。上述漏洞的综合评级为“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：http://www.cnvd.org.cn/flaw/show/CNVD-2018-14926
http://www.cnvd.org.cn/flaw/show/CNVD-2018-14927
http://www.cnvd.org.cn/flaw/show/CNVD-2018-14928
http://www.cnvd.org.cn/flaw/show/CNVD-2018-14929

http://www.cnvd.org.cn/flaw/show/CNVD-2018-14932

http://www.cnvd.org.cn/flaw/show/CNVD-2018-14930

http://www.cnvd.org.cn/flaw/show/CNVD-2018-14931

http://www.cnvd.org.cn/flaw/show/CNVD-2018-14933

3、Apple 产品安全漏洞

Apple iOS 是为移动设备所开发的一套操作系统。macOS 是为 Mac 系列产品开发的专属操作系统。Apple Safari 是一款 Web 浏览器，是 Mac OS X 和 iOS 操作系统附带的默认浏览器。Safari 是其中的一个用于 Safari 浏览器的专用组件。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞获取敏感信息，执行任意代码或发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Apple iOS Wi-Fi 内存破坏漏洞、Apple Safari 地址栏欺骗漏洞（CNVD-2018-14959）、Apple iOS 拒绝服务漏洞（CNVD-2018-14961）、Apple macOS/OS X 敏感信息泄露漏洞、Apple iOS 任意代码执行漏洞（CNVD-2018-14963）、Apple macOS/OS X 提权漏洞、Apple macOS/OS X 敏感信息泄露漏洞（CNVD-2018-14965）、Apple iOS 信息泄露漏洞（CNVD-2018-14968）。其中，“Apple iOS Wi-Fi 内存破坏漏洞、Apple iOS 任意代码执行漏洞（CNVD-2018-14963）、Apple macOS/OS X 提权漏洞”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：http://www.cnvd.org.cn/flaw/show/CNVD-2018-14957

http://www.cnvd.org.cn/flaw/show/CNVD-2018-14959

http://www.cnvd.org.cn/flaw/show/CNVD-2018-14961

http://www.cnvd.org.cn/flaw/show/CNVD-2018-14960

http://www.cnvd.org.cn/flaw/show/CNVD-2018-14963

http://www.cnvd.org.cn/flaw/show/CNVD-2018-14964

http://www.cnvd.org.cn/flaw/show/CNVD-2018-14965

http://www.cnvd.org.cn/flaw/show/CNVD-2018-14968

4、Mozilla 产品安全漏洞

Mozilla Firefox 是一款开源 Web 浏览器，Firefox ESR 是 Firefox 的一个延长支持版本。Thunderbird 是从 Mozilla Application Suite 中独立出来的一套电子邮件客户端软件。本周，该产品被披露存在多个漏洞，攻击者可利用漏洞越边界读取内存数据，执行任意代码或发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：多款 Mozilla 产品内存破坏漏洞、多款 Mozilla 产品越界写入漏洞、多款 Mozilla 产品越边界读取漏洞（CNVD-2018-14973）、多款 Mozilla 产品缓冲区溢出漏洞（CNVD-2018-14974）、多款 Mozilla 产品内存错误引用漏洞（CNVD-2018-14971、CNVD-2018-14972）、Mozilla Firefox 和 Firefox ESR 拒绝服务漏洞（CNVD-2018-14985）、Mozilla Firefox 和 Firefox ESR 内存破坏漏洞（CNVD-2018-14986）。

其中，除“多款 Mozilla 产品缓冲区溢出漏洞（CNVD-2018-14974）、Mozilla Firefox 和 Firefox ESR 拒绝服务漏洞（CNVD-2018-14985）”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：http://www.cnvd.org.cn/flaw/show/CNVD-2018-14969
http://www.cnvd.org.cn/flaw/show/CNVD-2018-14970
http://www.cnvd.org.cn/flaw/show/CNVD-2018-14973
http://www.cnvd.org.cn/flaw/show/CNVD-2018-14974
http://www.cnvd.org.cn/flaw/show/CNVD-2018-14971
http://www.cnvd.org.cn/flaw/show/CNVD-2018-14972
http://www.cnvd.org.cn/flaw/show/CNVD-2018-14985
http://www.cnvd.org.cn/flaw/show/CNVD-2018-14986

5、Samsung Syncthru Web Service 跨站请求伪造漏洞

Samsung Syncthru Web Service 是韩国三星（Samsung）公司的一款用于打印机的网络同步服务。本周，Samsung Syncthru Web Service 被披露存在跨站请求伪造漏洞。远程攻击者可利用该漏洞执行未授权的操作。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：http://www.cnvd.org.cn/flaw/show/CNVD-2018-14786

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.htm

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-2018-14694	Apache OpenWhisk 远程代码执行漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://lists.apache.org/thread.html/439bd5ff5822708c645a0d816ed9914b88c97eda32eae6ea211bc0dc@%3Cdev.openwhisk.apache.org%3E
CNVD-2018-14714	mruby 拒绝服务漏洞（CNVD-2018-14714）	高	厂商已发布漏洞修复程序，请及时关注更新：https://github.com/mruby/mruby/commit/b64ce17852b180dfeea81cf458660be41a78974d
CNVD-2018-14729	HP Ink Printers 远程代码执行漏洞（CNVD-2018-14729）	高	HP 官方已经发布了新版本固件修复了上述漏洞，请受影响的用户尽快升级进行防护：https://support.hp.com/us-en/document/c06097712
CNVD-201	Dell EMC Data Protection Ad	高	用户可联系供应商获得补丁信息：

8-14731	visor XML 外部实体漏洞		https://support.emc.com/downloads/829_Data-Protection-Advisor
CNVD-2018-14781	CFITSIO 存在多个缓冲区溢出漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：https://heasarc.gsfc.nasa.gov/fitsio/fitsio.html
CNVD-2018-14780	Cisco Prime Collaboration Provisioning 拒绝服务漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180801-pcp-dos
CNVD-2018-14784	Micro Focus GroupWise 任意文件上传漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：https://www.novell.com/support/kb/doc.php?id=7023223
CNVD-2018-14849	SAP NetWeaver 存在未明 SQL 注入漏洞（CNVD-2018-14849）	高	厂商已发布了漏洞修复程序，请及时关注更新：http://www.securityfocus.com/bid/100911/references
CNVD-2018-14867	OpenEMR 远程代码执行漏洞	高	用户可参考如下供应商提供的安全公告获得补丁信息：https://github.com/openemr/openemr/commit/a29465adebaacb67d65dc219e83fa2bd9eee79af#diff-b50be4e7e554bc8f858ee3f864562c31
CNVD-2018-15061	Google Chrome 越界内存写入漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：https://chromereleases.googleblog.com/2018/06/stable-channel-update-for-desktop_12.html

小结：本周，Foxit 被披露存在多个漏洞，攻击者可利用漏洞执行任意代码。此外，Adobe、Apple、Mozilla 等多款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，执行任意代码或发起拒绝服务攻击。另外，Samsung Syncthru Web Service 跨站请求伪造漏洞，远程攻击者可利用该漏洞执行未授权的操作。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。

本周漏洞要闻速递

1. Linux 内核出现漏洞可触发远程 DoS 攻击

Linux 内核 4.9 版本中出现一个漏洞，可被攻击者利用，通过网络工具套件发起 DoS 攻击。研究人员表示，有很多网络设备供应商、电脑和服务器制造商、移动供应商

以及操作系统制造商都可能受到影响。此外，由于 Linux 使用范围很广，亚马逊、苹果、Ubuntu 以及 ZyXEL 也都可能中招。漏洞目前命名为 SegementSmack，编号为 CVE-2018-5390，目前除了还未有效的缓解措施。

参考链接：https://www.zdnet.com/article/linux-kernel-bug-tcp-flaw-lets-remote-attackers-stall-devices-with-tiny-dos-attack/

2. 医疗实践管理软件 OpenEMR 曝 22 个漏洞，1 亿患者资料面临泄露风险

8 月 7 日，一组研究人员公开披露了存在于 OpenEMR 软件中的 22 个安全漏洞。OpenEMR 是一个被广泛使用的医疗实践管理软件，支持电子病历。在此次被披露的漏洞中，包括了一个门户身份验证绕过漏洞，允许攻击者访问任何患者的记录。

参考链接：https://www.easyaq.com/news/2023956100.shtml

关于 CNVD

国家信息安全漏洞共享平台（China National Vulnerability Database，简称 CNVD）是 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信息安全漏洞信息共享知识库，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，是我国网络安全应急体系的核心协调机构。

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