国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2018 年 1 月 29 日-2018 年 2 月 4 日 **2018 年第 5 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 382 个，其中高危漏洞 101 个、中危漏洞 244 个、低危漏洞 37 个。漏洞平均分值为 5.75。本周收录的漏洞中，涉及 0day 漏洞 64 个（占 17%），其中互联网上出现“MASTER IPCAMERA01 硬编码漏洞、ZyXEL P-660HW 拒绝服务漏洞”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 581 个，与上周（671）个环比降低 13%。

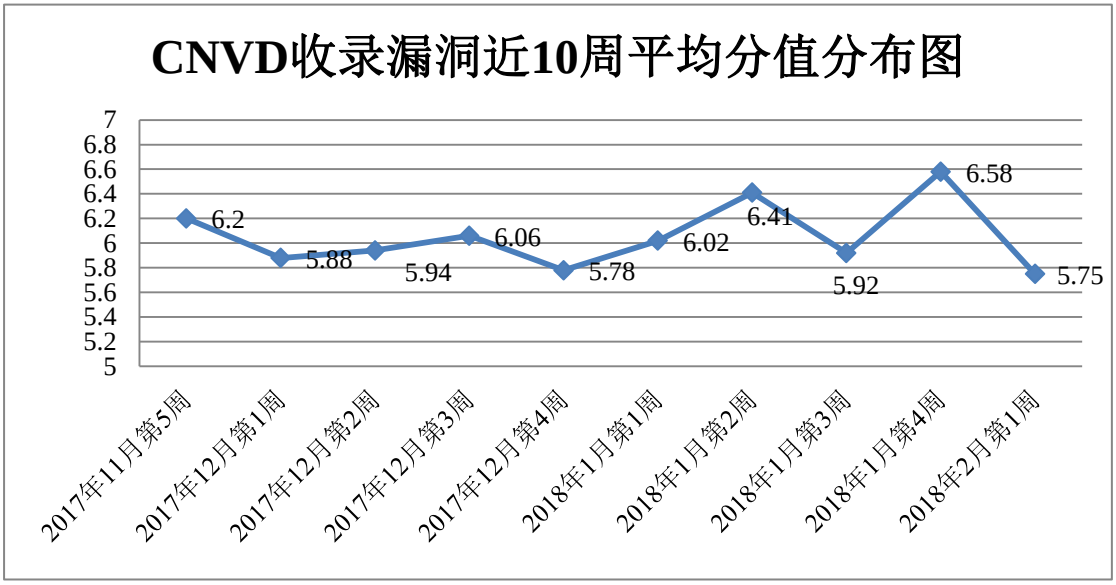

图 1 CNVD 收录漏洞近 10 周平均分值分布图

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，华为技术有限公司、安天实验室、启明星辰、天融信、H3C 等等单位自主挖掘或收集的数量较多。四川虹微技术有限公司（子午攻防实验室）、上海观安信息技术股份有限公司、南京联成科技发展股份有限公司、福建省海

峡信息技术有限公司、中新网络信息安全股份有限公司、杭州安信检测技术有限公司、聚锋信息安全实验室、上海银基信息安全技术股份有限公司及其他个人白帽子向 CNVD 提交了 581 个以事件型漏洞为主的原创漏洞。

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
360 网神(补天平台)	224	224
华为技术有限公司	225	0
安天实验室	188	0
启明星辰	148	4
天融信	136	4
H3C	113	0
恒安嘉新	83	2
卫士通信息产业股份有限公司	78	0
中国电信集团系统集成有限责任公司	62	0
漏洞盒子	59	59
绿盟科技	57	0
北京数字观星科技有限公司	49	0
杭州安恒信息技术有限公司	40	0
北京无声信息技术有限公司	6	0
知道创宇	3	3
东软	3	3
四川虹微技术有限公司（子午攻防实验室）	45	45
上海观安信息技术股份有限公司	21	21
南京联成科技发展股份有限公司	10	10

福建省海峡信息技术有限公司	9	9
中新网络信息安全股份有限公司	8	8
杭州安信检测技术有限公司	1	1
聚锋信息安全实验室	1	1
上海银基信息安全技术股份有限公司	1	1
CNCERT 吉林分中心	7	7
CNCERT 新疆分中心	6	6
CNCERT 河北分中心	3	3
CNCERT 江西分中心	3	3
CNCERT 广东分中心	3	3
CNCERT 陕西分中心	2	2
CNCERT 上海分中心	2	2
CNCERT 浙江分中心	1	1
个人	159	159
报送总计	1756	581

本周漏洞按类型和厂商统计

本周，CNVD 收录了 382 个漏洞。其中应用程序漏洞 233 个，WEB 应用漏洞 51 个，操作系统漏洞 28 个，网络设备漏洞 27 个，安全产品漏洞 24 个和数据库漏洞 19 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	233
WEB 应用漏洞	51
操作系统漏洞	28
网络设备漏洞	27
安全产品漏洞	24
数据库漏洞	19

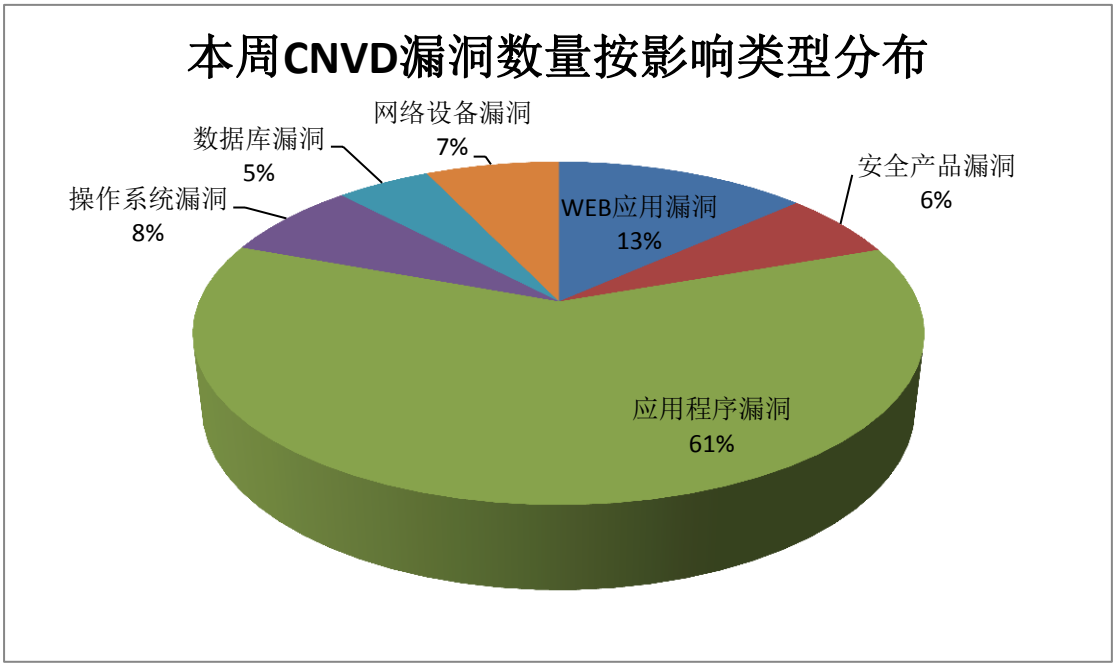

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Oracle、Mozilla、IBM 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	Oracle	87	23%
2	Mozilla	32	8%
3	IBM	17	4%
4	Apple	16	4%
5	Huawei	14	4%
6	Cisco	10	3%
7	Malwarebytes	10	3%
8	K7	10	2%
9	Google	8	2%
10	其他	178	47%

本周行业漏洞收录情况

本周，CNVD 收录了 29 个电信行业漏洞，28 个移动互联网行业漏洞，9 个工控行业漏洞（如下图所示）。其中，“Siemens TeleControl Server Basic 权限提升漏洞、ZyXEL P-660HW 拒绝服务漏洞、Oracle MySQL Server 存在未明漏洞（CNVD-2018-02163）、

多款 Apple 产品 QuartzCore 组件任意代码执行漏洞、Google Android Partition table updater 权限提升漏洞”等漏洞的综合评级为“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/

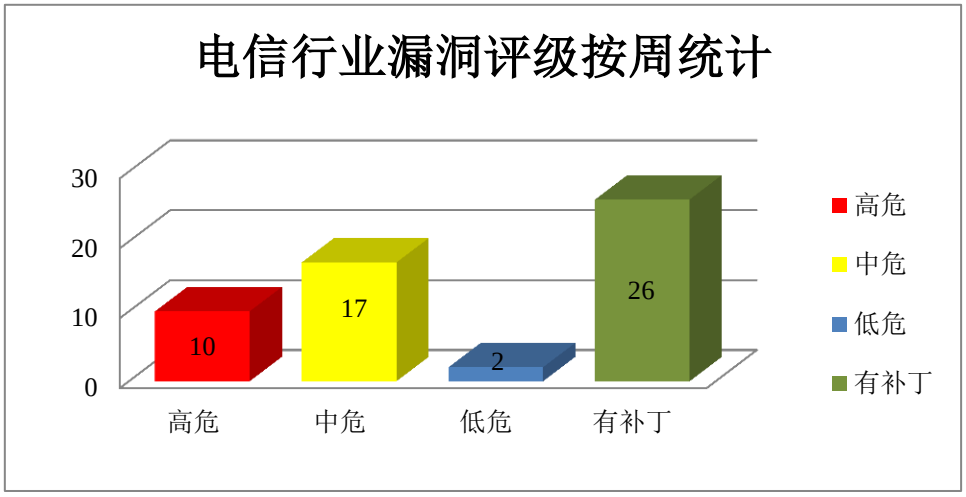

图 3 电信行业漏洞统计

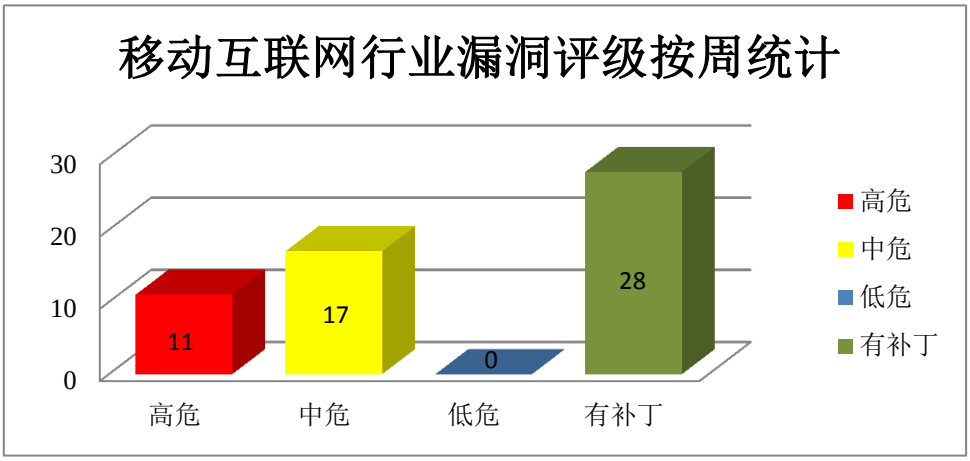

图 4 移动互联网行业漏洞统计

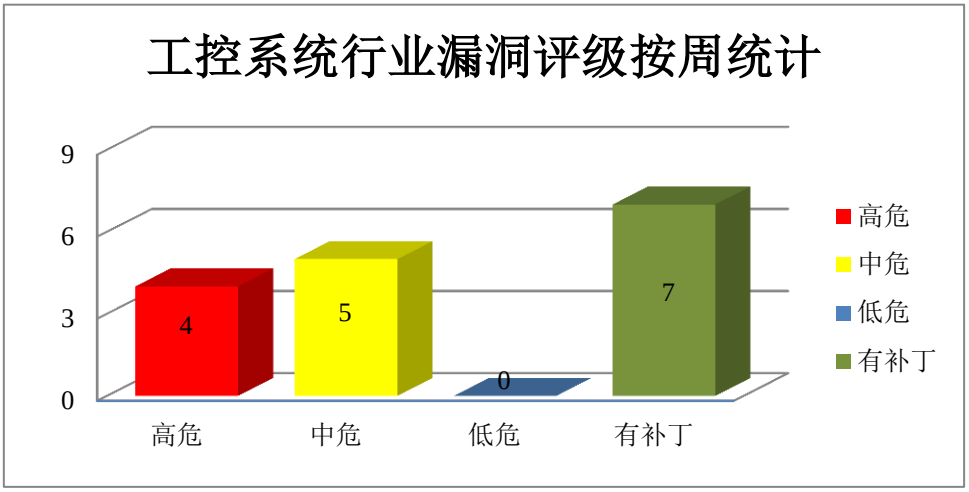

图 5 工控行业漏洞统计

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、PHP GD Graphics Library 拒绝服务漏洞

PHP 是一种通用开源脚本语言。GD Graphics Library（又名 libgd 或 libgd2）是一个开源的用于动态创建图像的库。本周，该产品被披露存在拒绝服务漏洞，攻击者可通过特制的 GIF 文件利用该漏洞造成拒绝服务（无限循环）。

CNVD 收录的相关漏洞包括：PHP GD Graphics Library 拒绝服务漏洞。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-2018-02505

2、Oracle 产品安全漏洞

Oracle MySQL 是美国甲骨文（Oracle）公司的一个小型关系型数据库管理系统。Oracle Java SE 是一套标准版 Java 平台。Oracle Sun Systems Products Suite 是 Sun 系统产品包。本周，上述产品被披露存在未明漏洞，攻击者可利用该漏洞影响机密性、完整性和可用性。

CNVD 收录的相关漏洞包括：Oracle MySQL Server 存在未明漏洞（CNVD-2018-02156、CNVD-2018-02163、CNVD-2018-02166、CNVD-2018-02165）、Oracle Java SE 存在未明漏洞（CNVD-2018-02254、CNVD-2018-02255）、Oracle Sun Systems Products Suite 存在未明漏洞（CNVD-2018-02523、CNVD-2018-02527）。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-2018-02156

http://www.cnvd.org.cn/flaw/show/CNVD-2018-02163

http://www.cnvd.org.cn/flaw/show/CNVD-2018-02166

http://www.cnvd.org.cn/flaw/show/CNVD-2018-02165

http://www.cnvd.org.cn/flaw/show/CNVD-2018-02254

http://www.cnvd.org.cn/flaw/show/CNVD-2018-02255

http://www.cnvd.org.cn/flaw/show/CNVD-2018-02523

http://www.cnvd.org.cn/flaw/show/CNVD-2018-02527

3、Mozilla 产品安全漏洞

Mozilla Firefox 和 Firefox ESR 都是美国 Mozilla 基金会开发的浏览器产品。本周，上述产品被披露存在内存破坏和内存错误引用漏洞，攻击者可利用漏洞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：Mozilla Firefox 和 Firefox ESR 内存破坏漏洞（CNVD-2018-02635）、Mozilla Firefox 内存破坏漏洞（CNVD-2018-02636）、Mozilla Firefox 和 Firefox ESR 内存错误引用漏洞（CNVD-2018-02637、CNVD-2018-02639、CNVD-2018-02640、CNVD-2018-02641、CNVD-2018-02644、CNVD-2018-02645）。其中“Mozilla Firefox 和 Firefox ESR 内存破坏漏洞（CNVD-2018-02635）、Mozilla Firefox 内存破坏漏洞（CNVD-2018-02636）”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-2018-02635

http://www.cnvd.org.cn/flaw/show/CNVD-2018-02636

http://www.cnvd.org.cn/flaw/show/CNVD-2018-02637

http://www.cnvd.org.cn/flaw/show/CNVD-2018-02639

http://www.cnvd.org.cn/flaw/show/CNVD-2018-02640

http://www.cnvd.org.cn/flaw/show/CNVD-2018-02641

http://www.cnvd.org.cn/flaw/show/CNVD-2018-02644

http://www.cnvd.org.cn/flaw/show/CNVD-2018-02645

4、IBM 产品安全漏洞

IBM Remote Control 是美国 IBM 公司的一款远程控制管理程序，IBM MQ 是一款消息传递中间件产品，IBM Rational DOORS 一套用于捕获、跟踪、分析和管理需求的软件，IBM Tealeaf Customer Experience 是一套基于 SaaS 的网络和移动应用分析解决方案。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系统的访问权限或向 Web UI 注入任意的 JavaScript 脚本。

CNVD 收录的相关漏洞包括：IBM Remote Control 权限提升漏洞、IBM MQ service trace 模块权限提升漏洞、IBM Rational DOORS Web Access 跨站脚本漏洞（CNVD-2018-02501、CNVD-2018-02502、CNVD-2018-02503）、IBM Rational DOORS Web Access 凭证存储漏洞、IBM Tealeaf Customer Experience 会话漏洞、IBM Tealeaf Custo

mer Experience 硬编码证书漏洞。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-2018-02690
http://www.cnvd.org.cn/flaw/show/CNVD-2018-02188
http://www.cnvd.org.cn/flaw/show/CNVD-2018-02501
http://www.cnvd.org.cn/flaw/show/CNVD-2018-02502
http://www.cnvd.org.cn/flaw/show/CNVD-2018-02503
http://www.cnvd.org.cn/flaw/show/CNVD-2018-02500
http://www.cnvd.org.cn/flaw/show/CNVD-2018-02372
http://www.cnvd.org.cn/flaw/show/CNVD-2018-02366

5、 Nari PCS-9611 relay 输入验证漏洞

Nari PCS-9611 relay 是中国国电南瑞（Nari）公司的一款线路保护测控设备。本周，Nari 被披露存在输入验证漏洞，攻击者可利用漏洞任意读取/访问系统资源。目前，厂商尚未发布漏洞修补程序。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：http://www.cnvd.org.cn/flaw/show/CNVD-2018-02349

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-2018-02146	K7 Antivirus Premium 权限提升漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://support.k7computing.com/index.php?/Knowledgebase/Article/View/176/41/advisory-issued-on-6th-november-2017
CNVD-2018-02172	Trustwave Secure Web Gateway 权限提升漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://www.trustwave.com/Resources/Trustwave-Software-Updates/Important-Security-Update-for-Trustwave-Secure-Web-Gateway/
CNVD-2018-02196	Apache OFBiz 代码注入漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：https://ofbiz.apache.org/
CNVD-2018-02230	Linux kernel 拒绝服务漏洞（CNVD-2018-02230）	高	目前厂商已发布漏洞修复程序，请及时关注更新：https://git.kernel.org/pub/scm/linux/kern

			el/git/torvalds/linux.git/commit/?id=2638fd0f92d4397884fd991d8f4925cb3f081901
CNVD-2018-02342	Gifsicle gifview 'read_gif'函数内存错误引用漏洞	高	目前厂商已发布漏洞修复程序，请及时关注更新：https://github.com/kohler/gifsicle/commit/81fd7823f6d9c85ab598bc850e40382068361185
CNVD-2018-02344	PHOENIX CONTACT mGuard 未授权修改漏洞	高	用户可联系供应商获得补丁信息：http://www.phoenixcontact.net/qr/2702547/firmware_update
CNVD-2018-02347	Siemens TeleControl Server Basic 权限提升漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：https://www.siemens.com/cert/pool/cert/siemens_security_advisory_ssa-651454.pdf
CNVD-2018-02362	Cisco D9800 Network Transport Receiver 命令注入漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180117-ntr
CNVD-2018-02367	IBM Tealeaf Customer Experience 任意文件读取漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：http://www-01.ibm.com/support/docview.wss?uid=swg22006392
CNVD-2018-02674	Primetek Primefaces 远程代码执行漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：https://github.com/primefaces/primefaces/commit/26e44eb7962cbdb6aa2f47eca0f230f3274358f0

小结：本周，PHP GD Graphics Library 拒绝服务漏洞，攻击者可通过特制的 GIF 文件利用该漏洞造成拒绝服务。此外，Oracle、Mozilla、IBM 等多款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、发起拒绝服务攻击或获取权限等。另外，Nari PCS-9611 被披露存在输入验证漏洞，攻击者可利用漏洞任意读取/访问系统资源。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. Adobe Flash 零日漏洞（cve-2018-4878）在野攻击

2 月 1 日， Adobe 官方发布了 Adobe Flash Player 系列产品的安全通告（APSA18-01），一个最新的 Adobe Flash 零日漏洞被发现针对韩国地区的人员发起攻击，该 0day

漏洞编号为 CVE-2018-4878，攻击者在 Office 文档、网页、垃圾邮件内嵌入恶意 Flash 实施攻击，用户打开文件或链接就会中招，目前最新版本 28.0.0.137 及其以前版本的 Adobe Flash Player 均受漏洞影响，Adobe 官方将于 2 月 5 日发布漏洞补丁。

参考链接：http://www.freebuf.com/vuls/162049.html

2. ManageEngine 企业级 IT 运维管理产品曝多个严重漏洞

网络安全公司 Digital Defense 的研究人员发现 ManageEngine 的企业级 IT 运维管理产品存在多个严重的漏洞，包括文件上传漏洞、盲目的 SQL 注入漏洞、远程代码执行漏洞和用户枚举漏洞。未经身份验证的攻击者可利用该漏洞上传 JavaScript Web Shell，借助 SYSTEM 权限执行任意命令。SQL 注入漏洞允许未经身份验证的攻击者完全控制应用程序，甚至控制底层主机。枚举漏洞允许攻击者访问用户信息；受未经身份验证的 XML 外部实体（XXE）注入漏洞影响，允许攻击者访问运行 ManageEngine 应用程序的主机上的文件内容。ManageEngine 已在其官网发布漏洞补丁。

参考链接：https://www.easyaq.com/news/303559774.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