# 国家信息安全漏洞共享平台(CNVD)

# 信息安全漏洞周报

2018 年 4 月 02 日-2018 年 4 月 08 日　　2018 年第 14 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 165 个，其中高危漏洞 44 个、中危漏洞 116 个、低危漏洞 5 个。漏洞平均分值为 5.97。本周收录的漏洞中，涉及 0day 漏洞 57 个（占 35%），其中互联网上出现“D-Link DIR-601 信息泄露漏洞、Rockwell Automation Allen Bradley Micrologix 1400 Series B FRN 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 562 个，与上周（391 个）环比增长 30%。

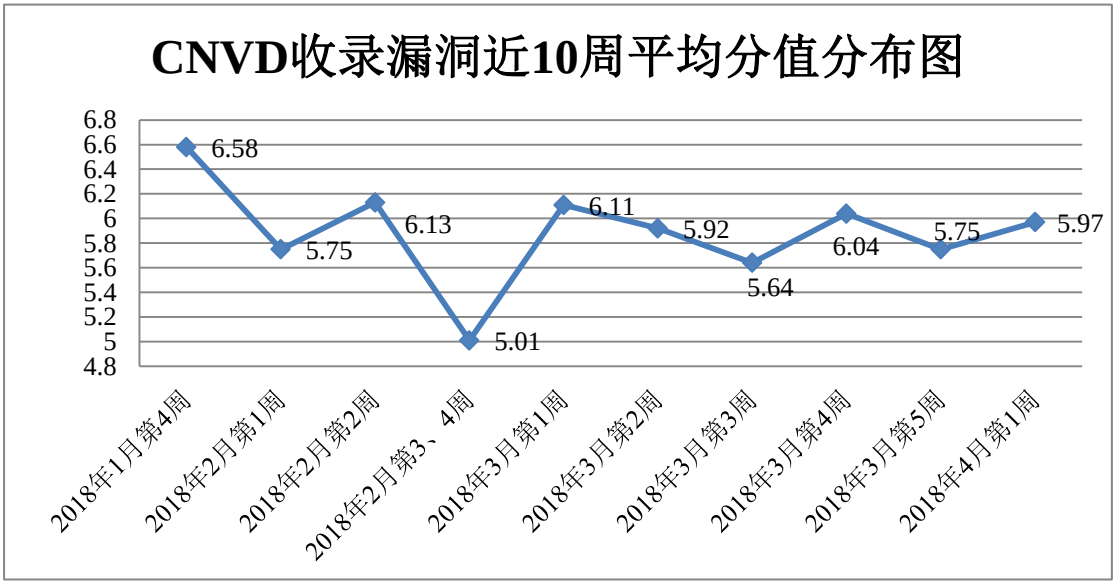


图 1 CNVD 收录漏洞近 10 周平均分值分布图

## 本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，北京启明星辰信息安全技术有限公司、哈尔滨安天科技股份有限公司、华为技术有限公司、北京天融信网络安全技术有限公司、北京数字观星科技有限公司等单位报送公开收集的漏洞数量较多。四川虹微技术有限公司（子午

攻防实验室）、中新网络信息安全股份有限公司、安徽锋刃信息科技有限公司、安徽三实信息技术服务有限公司、广西网信信息安全等级保护测评有限公司、南京联成科技发展股份有限公司、上海观安信息技术股份有限公司、广州万方计算机科技有限公司、漏斗社区、南瑞集团公司（国网电力科学研究院）及其他个人白帽子向 CNVD 提交了 562 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 373 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 |
|---|---|---|
| 漏洞盒子 | 215 | 215 |
| 北京启明星辰信息安全技术有限公司 | 185 | 0 |
| 360 网神（补天平台） | 158 | 158 |
| 哈尔滨安天科技股份有限公司 | 165 | 0 |
| 华为技术有限公司 | 118 | 0 |
| 北京天融信网络安全技术有限公司 | 86 | 2 |
| 北京数字观星科技有限公司 | 69 | 0 |
| 新华三技术有限公司 | 28 | 0 |
| 恒安嘉新(北京)科技股份公司 | 20 | 0 |
| 北京神州绿盟科技有限公司 | 15 | 0 |
| 卫士通信息产业股份有限公司 | 13 | 0 |
| 北京无声信息技术有限公司 | 7 | 0 |
| 中国电信集团系统集成有限责任公司 | 3 | 3 |
| 沈阳东软系统集成工程有限公司 | 1 | 1 |
| 四川虹微技术有限公司（子午攻防实验室） | 15 | 15 |
| 中新网络信息安全股份有限公司 | 11 | 11 |
| 安徽锋刃信息科技有限公司 | 6 | 6 |

| | | |
|---|---|---|
| 安徽三实信息技术服务有限公司 | 4 | 4 |
| 广西网信信息安全等级保护测评有限公司 | 4 | 4 |
| 南京联成科技发展股份有限公司 | 4 | 4 |
| 上海观安信息技术股份有限公司 | 4 | 4 |
| 广州万方计算机科技有限公司 | 1 | 1 |
| 漏斗社区 | 1 | 1 |
| 南瑞集团公司（国网电力科学研究院） | 1 | 1 |
| CNCERT 吉林分中心 | 2 | 2 |
| 个人 | 130 | 130 |
| 报送总计 | 1266 | 562 |

## 本周漏洞按类型和厂商统计

本周，CNVD 收录了 165 个漏洞。其中应用程序漏洞 116 个，WEB 应用漏洞 23 个，安全产品漏洞 16 个，网络设备漏洞 9 个，操作系统漏洞 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 | 116 |
| WEB 应用漏洞 | 23 |
| 安全产品漏洞 | 16 |
| 网络设备漏洞 | 9 |
| 操作系统漏洞 | 1 |

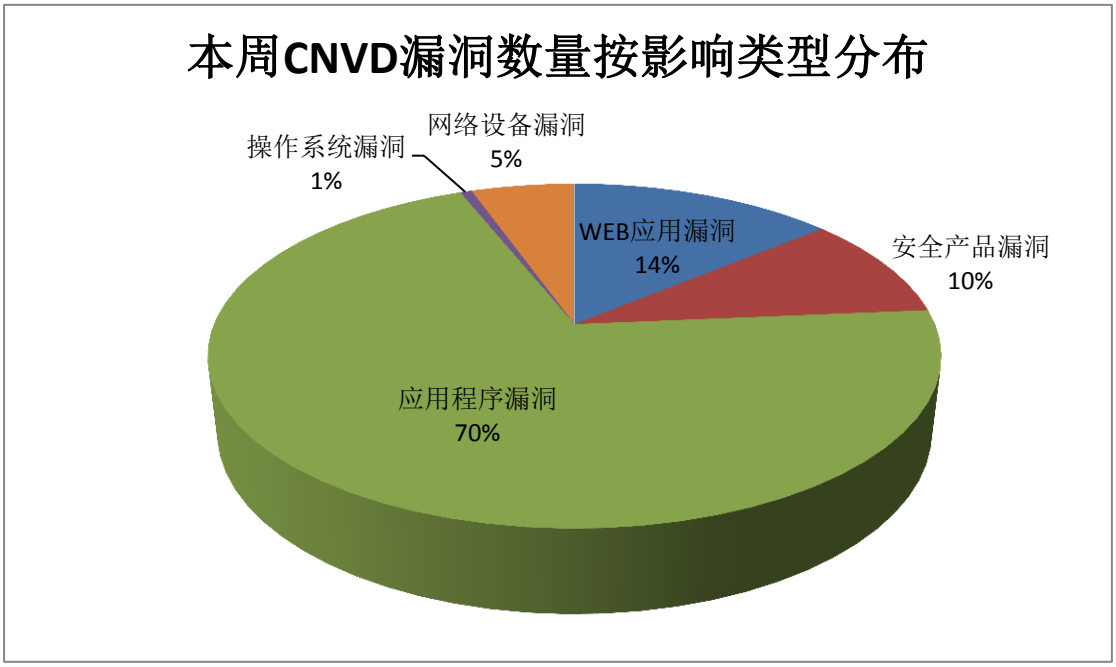


图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Windows Master、IObit、GitLab 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 | Windows Master | 20 | 12% |
| 2 | IObit | 15 | 9% |
| 3 | GitLab | 14 | 8% |
| 4 | Microsoft | 11 | 7% |
| 5 | mozilla | 10 | 6% |
| 6 | RubyGems | 6 | 4% |
| 7 | Dell | 4 | 2% |
| 8 | CA | 3 | 2% |
| 9 | GraphicsMagick | 3 | 2% |
| 10 | 其他 | 79 | 48% |

## 本周行业漏洞收录情况

本周，CNVD 收录了 6 个电信行业漏洞，8 个移动互联网行业漏洞，5 个工控行业漏洞（如下图所示）。其中，“Intel® 2G Modem firmware 缓冲区溢出漏洞、iemens SIMATIC 多款产品拒绝服务漏洞、Siemens TIM 1531 IRC 安全绕过漏洞”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/

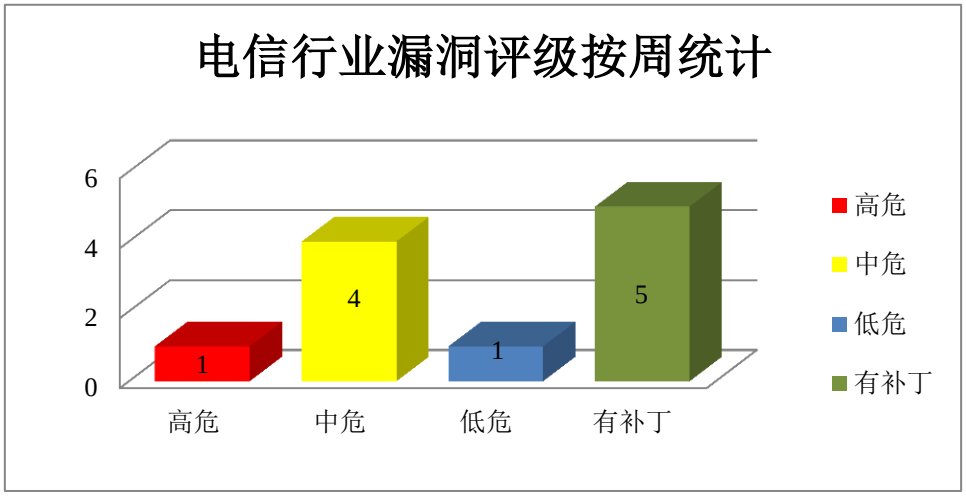


图 3 电信行业漏洞统计

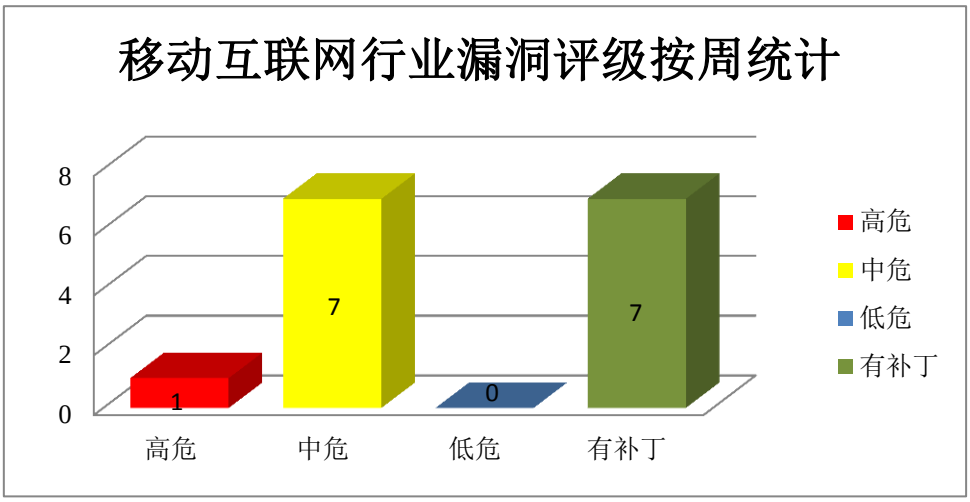


图 4 移动互联网行业漏洞统计

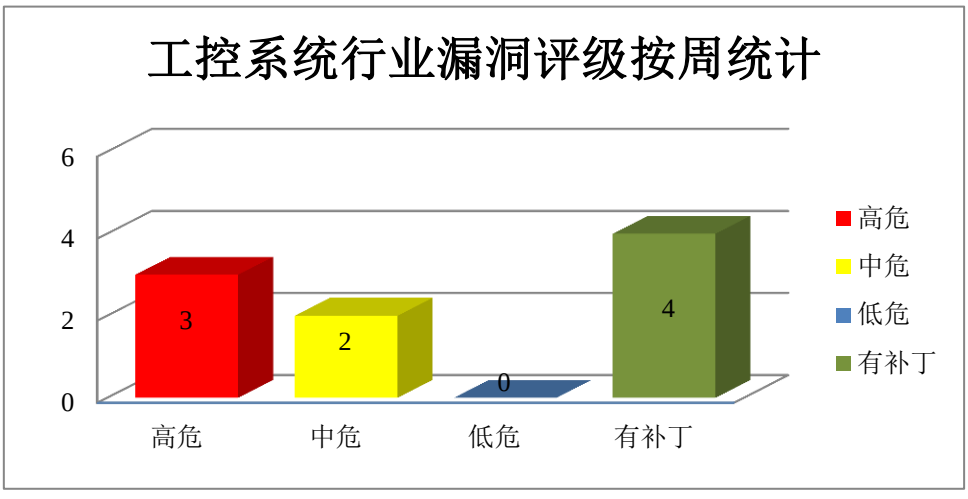

图 5 工控行业漏洞统计

## 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、Cisco Smart Install 远程命令执行漏洞

Smart Install 实现了自动化初始配置和操作系统镜像加载的过程，同时还提供配置文件的备份功能。本周，该产品被披露存在远程命令执行漏洞，攻击者可利用漏洞造成设备远程执行 Cisco 系统命令或拒绝服务（DoS）。

CNVD 收录的相关漏洞包括：Cisco Smart Install 远程命令执行漏洞。该漏洞的综合评级为“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-2018-06774

### 2、Microsoft 产品安全漏洞

Microsoft Project Server 是美国微软（Microsoft）公司的一套适用于项目组合管理（PPM）和日常工作的项目管理解决方案。SharePoint Enterprise Server 2016 是一套企业业务协作平台。本周，上述产品被披露存在远程权限提升漏洞，攻击者可利用漏洞提升权限。

CNVD 收录的相关漏洞包括：Microsoft SharePoint 远程权限提升漏洞（CNVD-2018-07004、CNVD-2018-07005、CNVD-2018-07006、CNVD-2018-07007、CNVD-2018-07008、CNVD-2018-07009、CNVD-2018-07010、CNVD-2018-07011）。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-2018-07004
http://www.cnvd.org.cn/flaw/show/CNVD-2018-07005
http://www.cnvd.org.cn/flaw/show/CNVD-2018-07006
http://www.cnvd.org.cn/flaw/show/CNVD-2018-07007
http://www.cnvd.org.cn/flaw/show/CNVD-2018-07008
http://www.cnvd.org.cn/flaw/show/CNVD-2018-07009
http://www.cnvd.org.cn/flaw/show/CNVD-2018-07010
http://www.cnvd.org.cn/flaw/show/CNVD-2018-07011

### 3、Iobit 产品安全漏洞

Advanced SystemCare Ultimate 是一套用于 Windows 系统的病毒防护软件。本周，该产品被披露存在拒绝服务漏洞，攻击者可利用漏执发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Advanced SystemCare Ultimate 拒绝服务漏洞（CNVD-2018-07108、CNVD-2018-07109、CNVD-2018-07110、CNVD-2018-07111、CNVD-20

18-07112、CNVD-2018-07113、CNVD-2018-07114、CNVD-2018-07115）。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-2018-07108
http://www.cnvd.org.cn/flaw/show/CNVD-2018-07109
http://www.cnvd.org.cn/flaw/show/CNVD-2018-07110
http://www.cnvd.org.cn/flaw/show/CNVD-2018-07111
http://www.cnvd.org.cn/flaw/show/CNVD-2018-07112
http://www.cnvd.org.cn/flaw/show/CNVD-2018-07113
http://www.cnvd.org.cn/flaw/show/CNVD-2018-07114
http://www.cnvd.org.cn/flaw/show/CNVD-2018-07115

### 4、Mozilla 产品安全漏洞

Mozilla Firefox 浏览器（火狐）是一个自由的、开放源码的浏览器，适用于 Windows、Linux 及 MacOSX 平台。本周，该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等。

CNVD 收录的相关漏洞包括：Mozilla Firefox 越界写入漏洞、Mozilla Firefox 缓冲区溢出漏洞（CNVD-2018-07092）、Mozilla Firefox 内存错误引用漏洞（CNVD-2018-07091）、Mozilla Firefox 内存破坏漏洞（CNVD-2018-07089）、Mozilla Firefox 信息泄露漏洞（CNVD-2018-07084、CNVD-2018-07085、CNVD-2018-07086、CNVD-2018-07087）。除“Mozilla Firefox 信息泄露漏洞（CNVD-2018-07084、CNVD-2018-07085、CNVD-2018-07086、CNVD-2018-07087）”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-2018-07090
http://www.cnvd.org.cn/flaw/show/CNVD-2018-07092
http://www.cnvd.org.cn/flaw/show/CNVD-2018-07091
http://www.cnvd.org.cn/flaw/show/CNVD-2018-07089
http://www.cnvd.org.cn/flaw/show/CNVD-2018-07084
http://www.cnvd.org.cn/flaw/show/CNVD-2018-07085
http://www.cnvd.org.cn/flaw/show/CNVD-2018-07086
http://www.cnvd.org.cn/flaw/show/CNVD-2018-07087

### 5、Rockwell Automation Allen Bradley Micrologix 1400 Series B FRN 拒绝服务漏洞

Rockwell Automation Allen Bradley Micrologix 1400 Series B FRN 是美国罗克韦尔（Rockwell Automation）公司的一款可编程逻辑控制器。本周，Rockwell Automation 被披露存在拒绝服务漏洞，攻击者可通过发送特制的数据包利用该漏洞造成设备进入

故障状态，删除梯形逻辑。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-2018-07012

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-2018-06863 | Unify OpenScape Deployment Service SQL 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://networks.unify.com/security/advisories/OBSO-1404-01.pdf |
| CNVD-2018-06882 | NPR Visuals Team Pym.js 跨站请求伪造漏洞 | 高 | 目前厂商已发布升级补丁以修复漏洞，补丁获取链接：http://blog.apps.npr.org/2018/02/15/pym-security-vulnerability.html |
| CNVD-2018-07036 | Siemens TIM 1531 IRC 安全绕过漏洞 | 高 | 目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://cert-portal.siemens.com/productcert/pdf/ssa-110922.pdf |
| CNVD-2018-07045 | Adobe Dreamweaver 任意代码执行漏洞 | 高 | 厂商已发布了漏洞修复程序，请及时关注更新：https://helpx.adobe.com/security/products/dreamweaver/apsb18-07.html |
| CNVD-2018-07049 | Red Hat CloudForms Management Engine 设计漏洞 | 高 | 目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://access.redhat.com/errata/RHSA-2018:0374 |
| CNVD-2018-07096 | Gitlab system_hook_push 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://about.gitlab.com/2018/01/16/gitlab-10-dot-3-dot-4-released/ |
| CNVD-2018-07097 | Gitlab GitlabProjectsImportService 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://about.gitlab.com/2018/01/16/gitlab-10-dot-3-dot-4-released/ |
| CNVD-2018-07098 | Gitlab SQL 注入漏洞 | 高 | 厂商已发布漏洞修复程序，请及时关注更新：https://about.gitlab.com/2018/01/16/gitlab-10-dot-3-dot-4-released/ |
| CNVD-2018-07101 | Gitlab project import 组件远程代码执行漏洞 | 高 | 厂商已发布漏洞修复程序，请及时关注更新： |

| | | | |
|---|---|---|---|
| | | | https://about.gitlab.com/2018/01/16/gitlab-10-dot-3-dot-4-released/ |
| CNVD-2018-07121 | Dell EMC ScaleIO 命令注入漏洞 | 高 | 厂商已发布漏洞修复程序，请及时关注更新：https://support.emc.com/downloads/40635_ScaleIO-Product-Family |

小结：本周，Cisco 被披露存在远程命令执行漏洞，攻击者可利用漏洞造成设备远程执行 Cisco 系统命令或拒绝服务（DoS）。此外，Microsoft、Iobit、Mozilla 等多款产品被披露存在多个漏洞，攻击者可利用漏洞泄露敏感信息、提升权限或发起拒绝服务攻击等。另外，Rockwell Automation 被披露存在拒绝服务漏洞，攻击者可通过发送特制的数据包利用该漏洞造成设备进入故障状态，删除梯形逻辑。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. 思科产品出现严重漏洞，导致大量设备面临远程攻击风险

思科 3 月 28 日发布安全公告指出，思科 IOS 和 IOS-XE 软件 Smart Install Client （开启了 Cisco Smart Install 管理协议，且模式为 client 模式）存在远程代码执行漏洞 CVE-2018-0171，CVSS 评分高达 9.8 分（总分 10 分）。攻击者可远程向 TCP 4786 端口发送恶意数据包，触发目标设备的栈溢出漏洞造成设备拒绝服务（DoS）或远程执行任意代码。

参考链接：https://www.easyaq.com/news/1791982842.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