# CNNVD漏洞分类指南

## 一、适用范围说明

凡是被国家信息安全漏洞库（CNNVD）收录的漏洞，均适用此分类规范，包括采集的公开漏洞以及收录的未公开漏洞，通用型漏洞及事件型漏洞。

## 二、漏洞类型

CNNVD将信息安全漏洞划分为26种类型，分别是：配置错误、代码问题、资源管理错误、数字错误、信息泄露、竞争条件、输入验证、缓冲区错误、格式化字符串、跨站脚本、路径遍历、后置链接、SQL注入、注入、代码注入、命令注入、操作系统命令注入、安全特征问题、授权问题、信任管理、加密问题、未充分验证数据可靠性、跨站请求伪造、权限许可和访问控制、访问控制错误、资料不足。

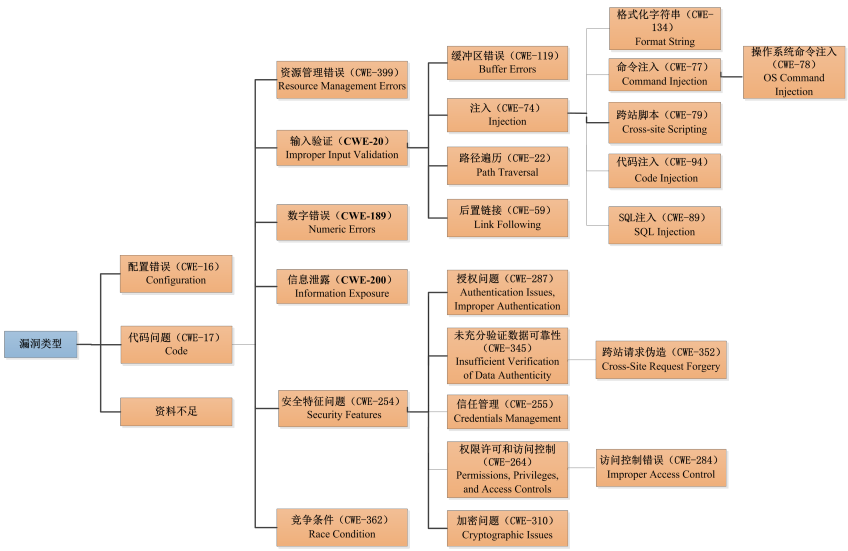


图1 漏洞分类层次树

图1给出了漏洞类型的层次关系。该分类模型包含多个抽象级别，高级别漏洞类型可以包含多个子级别，低级别的漏洞类型提供较细粒度的分类。

## 三、漏洞类型描述

### 1. 配置错误（CWE-16: Configuration）

#### 1.1 描述

此类漏洞指软件配置过程中产生的漏洞。该类漏洞并非软件开发过程中造成的，不存在于软件的代码之中，是由于软件使用过程中的不合理配置造成的。

#### 1.2 漏洞实例

（1）CNNVD-201606-433

漏洞名称：SolarWinds Virtualization Manager 安全漏洞

漏洞简介：

Solarwinds Virtualization Manager是美国SolarWinds公司的一套用于对虚拟化产品进行管理和监控的软件。该软件提供容量管理、性能监控和配置管理等功能。

SolarWinds Virtualization Manager 6.3.1及之前版本中存在安全漏洞。本地攻击者可借助sudo的错误配置利用该漏洞获取权限。

（2）CNNVD-201602-395

漏洞名称：Digium Asterisk Open Source和Certified Asterisk 拒绝服务漏洞

漏洞简介：

Digium Asterisk Open Source和Certified Asterisk都是美国Digium公司的开源电话交换机（PBX）系统软件。该软件支持语音信箱、多方语音会议、交互式语音应答(IVR)等。

Digium Asterisk Open Source和Certified Asterisk的chan_sip中存在安全漏洞。当timert1 sip.conf配置为大于1245的值时，远程攻击者可利用该漏洞造成拒绝服务（文件描述符消耗）。以下产品及版本受到影响：Digium Asterisk Open Source 1.8.x版本，11.21.1之前11.x版本，12.x版本，13.7.1之前13.x版本，Certified Asterisk 1.8.28版本，11.6-cert12之前11.6版本，13.1-cert3之前13.1版本。

（3）CNNVD-201410-618

漏洞名称：Apple OS X 配置错误漏洞

漏洞简介：

Apple OS X是美国苹果（Apple）公司为Mac计算机所开发的一套专用操作系统。

Apple OS X 10.10之前版本的MCX Desktop Config Profiles实现中存在安全漏洞，该漏洞源于程序保留已卸载mobile-configuration配置文件中的web-proxy设置。远程攻击者可通过访问代理服务器利用该漏洞获取敏感信息。

**2. 代码问题（CWE-17: Code）**

**2.1 描述**

此类漏洞指代码开发过程中产生的漏洞，包括软件的规范说明、设计和实现。该漏洞是一个高级别漏洞，如果有足够的信息可进一步分为更低级别的漏洞。

**2.2 与其他漏洞类型关系**

下级漏洞类型：资源管理错误（CWE-399）、输入验证（CWE-20）、数字错误（CWE-189）、信息泄露（CWE-200）、安全特征问题（CWE-254）、竞争条件（CWE-362）

**2.3 漏洞实例**

（1）CNNVD-201501-351

漏洞名称：Django 拒绝服务漏洞

漏洞简介：

Django是Django软件基金会的一套基于Python语言的开源Web应用框架。该框架包括面向对象的映射器、视图系统、模板系统等。

Django 1.6.10之前1.6.x版本和1.7.3之前1.7.x版本的ModelMultipleChoiceField中存在安全漏洞。当程序将show_hidden_initial设置为‘true’时，远程攻击者可通过提交重复的值利用该漏洞造成拒绝服务。

（2）CNNVD-201504-006

漏洞名称：Mozilla Firefox Off Main Thread Compositing 代码注入漏洞

漏洞简介：

Mozilla Firefox是美国Mozilla基金会开发的一款开源Web浏览器。

Mozilla Firefox 36.0.4及之前版本的Off Main Thread Compositing(OMTC)实现过程中存在安全漏洞，该漏洞源于程序与‘mozilla::layers::BufferTextureClient::AllocateForSurface’函数交互时，执行不正确的memset调用。远程攻击者可通过触发2D图形内容的渲染利用该漏洞执行任意代码，或造成拒绝服务（内存损坏和应用程序崩溃）。

分类关键因素：该漏洞源于程序与‘mozilla::layers::BufferTextureClient::AllocateForSurface’函数交互时，执行不正确的memset调用。

（3）CNNVD-201505-589

漏洞名称：Network Block Device 拒绝服务漏洞

漏洞简介：

Network Block Device（NBD，网络磁盘设备）是一套开源的网络存储软件。该软件能够创建基于Linux平台的网络存储系统。

NBD 3.11之前版本的nbd-server.c文件中存在安全漏洞，该漏洞源于程序没有正确处理信号。远程攻击者可利用该漏洞造成拒绝服务（死锁）。

**3. 资源管理错误（CWE-399: Resource Management Errors）**

**3.1 描述**

此类漏洞与系统资源的管理不当有关。该类漏洞是由于软件执行过程中对系统资源（如内存、磁盘空间、文件等）的错误管理造成的。

**3.2 与其他漏洞类型关系**

上级漏洞类型：代码（CWE-17）

**3.3 漏洞实例**

（1）CNNVD-201512-512

漏洞名称：Xen libxl toolstack库资源管理错误漏洞

漏洞简介：

Xen是英国剑桥大学开发的一款开源的虚拟机监视器产品。该产品能够使不同和不兼容的操作系统运行在同一台计算机上，并支持在运行时进行迁移，保证正常运行并且避免宕机。

Xen 4.1.x版本至4.6.x版本的libxl toolstack库中存在安全漏洞，该漏洞源于程序管理同一个进程中的多个域时没有正确释放做为内核和初始虚拟磁盘的文件映射。攻击者可通过启动域利用该漏洞造成拒绝服务（内存和磁盘资源消耗）。

（2）CNNVD-201505-312

漏洞名称：PHP 资源管理错误漏洞

漏洞简介：

PHP（PHP：Hypertext Preprocessor，PHP：超文本预处理器）是PHP Group和开放源代码社区共同维护的一种开源的通用计算机脚本语言。该语言支持多重语法、支持多数据库及操作系统和支持C、C++进行程序扩展等。

PHP的ext/phar/phar.c文件中的‘phar_parse_metadata’函数存在安全漏洞。远程攻击者可借助特制的tar归档利用该漏洞造成拒绝服务（堆元数据损坏）。以下版本受到影响:PHP 5.4.40之前版本，5.5.24之前5.5.x版本，5.6.8之前5.6.x版本。

（3）CNNVD-201502-440

漏洞名称：Mozilla Firefox WebGL 资源管理错误漏洞

漏洞简介：

Mozilla Firefox是美国Mozilla基金会开发的一款开源Web浏览器。

Mozilla Firefox 35.0.1及之前版本的WebGL实现过程中存在安全漏洞，该漏洞源于程序向shader的编译日志中复制字符串时，没有正确分配内存。远程攻击者可借助特制的WebGL内容利用该漏洞造成拒绝服务（应用程序崩溃）。

**4. 数字错误（CWE-189: Numeric Errors）**

**4.1 描述**

此类漏洞与不正确的数字计算或转换有关。该类漏洞主要由数字的不正确处理造成的，如整数溢出、符号错误、被零除等。

**4.2 与其他漏洞类型关系**

上级漏洞类型：代码问题（CWE-17）

**4.3 漏洞实例**

（1）CNNVD-201511-069

漏洞名称：Google Picasa 数字错误漏洞

漏洞简介：

Google Picasa是美国谷歌（Google）公司的一套免费的图片管理工具。该工具可协助用户在计算机上查找、修改和共享图片。

Google Picasa 3.9.140 Build 239版本和Build 248版本中存在整数溢出漏洞。远程攻击者可借助与‘phase one 0x412’标签相关的数据利用该漏洞执行任意代码。

（2）CNNVD-201509-592

漏洞名称：Android libstagefright 数字错误漏洞

漏洞简介：

Google Chrome是美国谷歌（Google）公司开发的一款Web浏览器。Android是美国谷歌（Google）公司和开放手持设备联盟（简称OHA）共同开发的一套以Linux为基础的开源操作系统。libstagefright是其中的一个硬解码支持库。

Android 4.4.4及之前版本的libstagefright中的SampleTable.cpp文件中存在整数溢出漏洞。攻击者可利用该漏洞造成拒绝服务（崩溃）。

（3）CNNVD-201503-502

漏洞名称：tcpdump‘mobility_opt_print’函数数字错误漏洞

漏洞简介：

tcpdump是Tcpdump团队开发的一套运行在命令行下的嗅探工具。该工具允许用户拦截和显示发送或收到过网络连接到该计算机的TCP/IP和其他数据包。

tcpdump 4.7.2之前版本的IPv6 mobility打印机（IPv6 mobility printer）中的‘mobility_opt_print’函数存在整数符号错误漏洞。远程攻击者可借助负的‘length’值利用该漏洞造成拒绝服务（越边界读取和崩溃），或执行任意代码。

**5. 信息泄露（CWE-200: Information Exposure）**

**5.1 描述**

信息泄露是指有意或无意地向没有访问该信息权限者泄露信息。此类漏洞是由于软件中的一些不正确的设置造成的信息泄漏。信息指（1）产品自身功能的敏感信息，如私有消息（2）或者有关产品或其环境的信息，这些信息可能在攻击中很有用，但是攻击者通常不能获取这些信息。信息泄露涉及多种不同类型的问题，并且严重程度依赖于泄露信息的类型。

**5.2 常见后果**

技术影响：Read application data

影响范围：机密性

**5.3 与其他漏洞类型关系**

上级漏洞类型：代码问题（CWE-17）

**5.4 漏洞实例**

（1）CNNVD-200412-094

漏洞名称：Linux Kernel USB驱动程序未初始化结构信息披露漏洞

漏洞简介：

Linux 2.4内核的Certain USB驱动程序使用未初始化结构中的copy_to_user功能，本地用户利用该漏洞通过读取内存获取敏感信息，该内存在以前使用后不曾被删除。

（2）CNNVD-200412-028

漏洞名称：Qbik WinGate信息披露漏洞

漏洞简介：

WinGate 5.2.3 build 901和6.0beta 2 build 942及如：5.0.5的其他版本存在漏洞。远程攻击者借助wingate-内部目录的URL请求读取根目录的任意文件。

（3）CNNVD-200412-415

漏洞名称：Microsoft Outlook Express BCC字段信息披露漏洞

漏洞简介：

Outlook Express 6.0版本在使用"Break apart messages larger than"设定发送分段邮件信息时，将消息的BBC收件人泄露到To及CC字段中地址，远程攻击者可能获得敏感信息。

**6. 竞争条件（CWE-362: Race Condition）**

**6.1 描述**

程序中包含可以与其他代码并发运行的代码序列，且该代码序列需要临时地、互斥地访问共享资源。但是存在一个时间窗口，在这个时间窗口内另一段代码序列可以并发修改共享资源。

如果预期的同步活动位于安全关键代码，则可能带来安全隐患。安全关键代码包括记录用户是否被认证，修改重要状态信息等。竞争条件发生在并发环境中，根据上下文，代码序列可以以函数调用，少量指令，一系列程序调用等形式出现。

**6.2 常见后果**

技术影响：DoS: resource consumption (CPU); DoS: resource consumption (memory); DoS: resource consumption (other); DoS: crash / exit / restart; DoS: instability; Read files or directories; Read application data

影响范围：机密性、完整性和可用性

**6.3 与其他漏洞类型关系**

上级漏洞类型：代码问题（CWE-17）

**6.4 漏洞实例**

（1）CNNVD-201505-221

漏洞名称：Mozilla Firefox‘nsThreadManager::RegisterCurrentThread’函数竞争条件漏洞

漏洞简介：

Mozilla Firefox是美国Mozilla基金会开发的一款开源Web浏览器。

Mozilla Firefox 37.0.2及之前版本的‘nsThreadManager::RegisterCurrentThread’函数中存在竞争条件漏洞，该漏洞源于程序执行关闭操作时，没有正确创建Media Decoder线程。远程攻击者可利用该漏洞执行任意代码，或造成拒绝服务（释放后重用和堆内存损坏）。

（2）CNNVD-201504-562

漏洞名称：IBM WebSphere Application Server Liberty Profile 竞争条件漏洞

漏洞简介：

IBM WebSphere Application Server（WAS）是美国IBM公司开发并发行的一款应用服务器产品，它是Java EE和Web服务应用程序的平台，也是IBM WebSphere软件平台的基础。Liberty Profile是WAS的一个动态服务器配置文件。

IBM WAS Liberty Profile 8.5版本中存在竞争条件漏洞。远程攻击者可利用该漏洞获取提升的权限。

（3）CNNVD-201502-268

漏洞名称：Cisco IOS MACE 安全漏洞

漏洞简介：

Cisco IOS是美国思科（Cisco）公司为其网络设备开发的操作系统。Measurement, Aggregation, and Correlation Engine（MACE）是其中的一个用于测量和分析网络报文的功能。

Cisco IOS 15.4(2)T3及之前版本的MACE实现过程中存在竞争条件漏洞。远程攻击者可借助特制的网络流量利用该漏洞造成拒绝服务（设备重载）。

**7. 输入验证（CWE-20: Improper Input Validation）**

**7.1 描述**

产品没有验证或者错误地验证可以影响程序的控制流或数据流的输入。如果有足够的信息，此类漏洞可进一步分为更低级别的类型。

当软件不能正确地验证输入时，攻击者能够伪造非应用程序所期望的输入。这将导致系统接收部分非正常输入，攻击者可能利用该漏洞修改控制流、控制任意资源和执行任意代码。

**7.2 常见后果**

技术影响：DoS: crash / exit / restart; DoS: resource consumption (CPU); DoS: resource consumption (memory)；Read memory; Read files or directories；Modify memory; Execute unauthorized code or commands

影响范围：机密性、完整性和可用性

**7.3 与其他漏洞类型关系**

上级漏洞类型：代码问题（CWE-17）

下级漏洞类型：缓冲区错误（CWE-119）、注入（CWE-74）、路径遍历（CWE-22）、后置链接（CWE-59）

**7.4 漏洞实例**

（1）CNNVD-201607-976

漏洞名称：Cisco Unified Computing System Performance Manager 输入验证漏洞

漏洞简介：

Cisco Unified Computing System（UCS）Performance Manager是美国思科（Cisco）公司的一套UCS组件性能监控软件。

Cisco UCS Performance Manager 2.0.0及之前的版本Web框架中存在输入验证漏洞。远程攻击者可通过发送特制的HTTP GET请求利用该漏洞执行任意命令。

（2）CNNVD-201606-360

漏洞名称：Adobe Brackets 输入验证漏洞

漏洞简介：

Adobe Brackets是美国奥多比（Adobe）公司的一套开源的基于HTML/CSS/JavaScript开发并运行于native shell上的集成开发环境。

基于Windows、Macintosh和Linux平台的Adobe Brackets 1.6及之前版本的扩展管理器中存在输入验证漏洞。攻击者可利用该漏洞造成未知影响。

（3）CNNVD-201512-474

漏洞名称：Mozilla Firefox 输入验证漏洞

漏洞简介：

Mozilla Firefox是美国Mozilla基金会开发的一款开源Web浏览器。

Mozilla Firefox 42.0及之前版本中存在安全漏洞，该漏洞源于程序没有正确处理data: URI中的‘#’字符。远程攻击者可利用该漏洞伪造Web站点。

**8. 缓冲区错误（CWE-119: Buffer Errors）**

**8.1 描述**

软件在内存缓冲区上执行操作，但是它可以读取或写入缓冲区的预定边界以外的内存位置。

某些语言允许直接访问内存地址，但是不能自动确认这些内存地址是有效的内存缓冲区。这可能导致在与其他变量、数据结构或内部程序数据相关联的内存位置上执行读/写操作。作为结果，攻击者可能执行任意代码、修改预定的控制流、读取敏感信息或导致系统崩溃。

**8.2 常见后果**

技术影响：Execute unauthorized code or commands; Modify memory；Read memory; DoS: crash / exit / restart; DoS: resource consumption (CPU); DoS: resource consumption (memory)

影响范围：机密性、完整性和可用性

**8.3 与其他漏洞类型关系**

上级漏洞类型：输入验证（CWE-20）

**8.4 漏洞实例**

（1）CNNVD-201608-309

漏洞名称：Cracklib 基于栈的缓冲区溢出漏洞

漏洞简介：

Linux-PAM（又名PAM）是一种用于Linux平台中的认证机制，它通过提供一些动态链接库和一套统一的API，使系统管理员可以自由选择应用程序使用的验证机制。Cracklib是其中的一个用于检查密码是否违反密码字典的模块。

Cracklib中的lib/fascist.c文件中的‘FascistGecosUser’函数存在基于堆的缓冲区溢出漏洞。本地攻击者可借助长的GECOS字段利用该漏洞造成拒绝服务（应用程序崩溃），或获取权限。

（2）CNNVD-201608-446

漏洞名称：Fortinet FortiOS和FortiSwitch 缓冲区溢出漏洞

漏洞简介：

Fortinet FortiOS和FortiSwitch都是美国飞塔（Fortinet）公司开发的产品。前者是一套专用于FortiGate网络安全平台上的安全操作系统，后者是一套专门用于以太网基础架构和现行网络边缘配置的安全交换平台。

Fortinet FortiOS和FortiSwitch中的Cookie解析器存在缓冲区溢出漏洞。远程攻击者可通过发送特制的HTTP请求利用该漏洞执行任意代码。以下版本受到影响：Fortinet FortiOS 4.1.11之前的4.x版本，4.2.13之前的4.2.x版本，4.3.9之前的4.3.x版本，FortiSwitch 3.4.3之前的版本。

（3）CNNVD-201606-184

漏洞名称：Red Hat SPICE 基于堆的缓冲区溢出漏洞

漏洞简介：

Red Hat SPICE是美国红帽（Red Hat）公司的一个企业虚拟化桌面版所使用的自适应远程呈现开源协议，它主要用于将用户与其虚拟桌面进行连接，能够提供与物理桌面完全相同的最终用户体验。

Red Hat SPICE的smartcard交互中存在基于堆的缓冲区溢出漏洞。攻击者可利用该漏洞造成拒绝服务（QEMU进程崩溃），或执行任意代码。

**9. 格式化字符串（CWE-134: Format String Vulnerability）**

**9.1 描述**

软件使用的函数接收来自外部源代码提供的格式化字符串作为函数的参数。

当攻击者能修改外部控制的格式化字符串时，这可能导致缓冲区溢出、拒绝服务攻击或者数据表示问题。

**9.2 常见后果**

技术影响：Read memory; Execute unauthorized code or commands

影响范围：机密性、完整性和可用性

**9.3 与其他漏洞类型关系**

上级漏洞类型：注入（CWE-74）

**9.4 漏洞实例**

（1）CNNVD-201512-593

漏洞名称：PHP 格式化字符串漏洞

漏洞简介：

PHP（PHP：Hypertext Preprocessor，PHP：超文本预处理器）是PHP Group和开放源代码社区共同维护的一种开源的通用计算机脚本语言。该语言支持多重语法、支持多数据库及操作系统和支持C、C++进行程序扩展等。

PHP 7.0.1之前7.x版本的Zend/zend_execute_API.c文件中的‘zend_throw_or_error’函数中存在格式化字符串漏洞。远程攻击者可借助不存在的类名中的格式字符串说明符利用该漏洞执行任意代码。

（2）CNNVD-201504-380

漏洞名称：Six Apart Movable Type 格式化字符串漏洞

漏洞简介：

Six Apart Movable Type（MT）是美国Six Apart公司的一套博客（blog）系统。Pro、Open Source和Advanced分别是该系统的专业版、开源版和高级版。

Six Apart MT中存在格式化字符串漏洞。远程攻击者可利用该漏洞执行任意代码。以下版本受到影响：Six Apart MT Pro 6.0.x版本和5.2.x版本，Open Source 5.2.x版本，Advanced 6.0.x版本和5.2.x版本。

（3）CNNVD-201404-001

漏洞名称：War FTP Daemon 格式化字符串漏洞

漏洞简介：

War FTP Daemon（warftpd）是一款用于Windows平台中的免费FTP服务器，它支持多重连接、用户权限设置和磁盘配额限制等。

warftpd 1.82 RC 12版本中存在格式化字符串漏洞。远程授权的攻击者可借助LIST命令中的格式字符串说明符利用该漏洞造成拒绝服务（崩溃）。

**10. 跨站脚本（CWE-79: Cross-site Scripting）**

**10.1 描述**

在用户控制的输入放置到输出位置之前软件没有对其中止或没有正确中止，这些输出用作向其他用户提供服务的网页。

跨站脚本漏洞通常发生在（1）不可信数据进入网络应用程序，通常通过网页请求；（2）网络应用程序动态地生成一个带有不可信数据的网页；（3）在网页生成期间，应用程序不能阻止Web浏览器可执行的内容数据，例如JavaScript，HTML标签，HTML属性、鼠标事件、Flash、ActiveX等；（4）受害者通过浏览器访问的网页包含带有不可信数据的恶意脚本；（5）由于脚本来自于通过web服务器发送的网页，因此受害者的web浏览器会在web服务器域的上下文中执行恶意脚本；（6）违反web浏览器的同源策略，同源策略是一个域中的脚本不能访问或运行其他域中的资源或代码。

**10.2 常见后果**

技术影响：Bypass protection mechanism; Read application data；Execute unauthorized code or commands

影响范围：机密性、完整性和可用性

**10.3 与其他漏洞类型关系**

上级漏洞类型：注入（CWE-74）

**10.4 漏洞实例**

（1）CNNVD-201611-004

漏洞名称：Cisco Prime Collaboration Provisioning 跨站脚本漏洞

漏洞简介：

Cisco Prime Collaboration Provisioning是美国思科（Cisco）公司的一套基于Web的下一代通信服务解决方案。该方案对IP电话、语音邮件和统一通信环境提供IP通信服务功能。

Cisco Prime Collaboration Provisioning的Web框架代码存在跨站脚本漏洞。远程攻击者可利用该漏洞在受影响网站上下文中注入任意脚本代码，访问敏感的browser-based信息。

（2）CNNVD-201609-096

漏洞名称：Fortinet FortiWAN 跨站脚本漏洞

漏洞简介：

Fortinet FortiWAN是美国飞塔（Fortinet）公司开发的一款广域网链路负载均衡产品。

Fortinet FortiWAN 4.2.4及之前的版本中存在跨站脚本漏洞。远程攻击者可通过向script/statistics/getconn.php脚本传递IP参数利用该漏洞注入任意Web脚本或HTML。

（3）CNNVD-201603-235

漏洞名称：Apache Struts I18NInterceptor 跨站脚本漏洞

漏洞简介：

Apache Struts是美国阿帕奇（Apache）软件基金会负责维护的一个开源项目，是一套用于创建企业级Java Web应用的开源MVC框架，主要提供两个版本框架产品，Struts 1和Struts 2。I18NInterceptor是使用在其中的一个国际化拦截器。

Apache Struts 2.3.25之前2.x版本的I18NInterceptor中存在跨站脚本漏洞，该漏洞源于程序没有充分过滤Locale对象中的文本。远程攻击者可利用该漏洞注入任意Web脚本或HTML。

**11. 路径遍历（CWE-22: Path Traversal）**

**11.1 描述**

为了识别位于受限的父目录下的文件或目录，软件使用外部输入来构建路径。由于软件不能正确地过滤路径中的特殊元素，能够导致访问受限目录之外的位置。

许多文件操作都发生在受限目录下。攻击者通过使用特殊元素（例如，“..”、“/”）可到达受限目录之外的位置，从而获取系统中其他位置的文件或目录。相对路径遍历是指使用最常用的特殊元素“../”来代表当前目录的父目录。绝对路径遍历（例如"/usr/local/bin"）可用于访问非预期的文件。

**11.2 常见后果**

技术影响：Execute unauthorized code or commands；Modify files or directories；Read files or directories；DoS: crash / exit / restart

影响范围：机密性、完整性和可用性

**11.3 与其他漏洞类型关系**

上级漏洞类型：输入验证（CWE-20）

**11.4 漏洞实例**

（1）CNNVD-201509-379

漏洞名称：GE Digital Energy MDS PulseNET和MDS PulseNET Enterprise 绝对路径遍历漏洞

漏洞简介：

GE Digital Energy MDS PulseNET和MDS PulseNET Enterprise都是美国通用电气（GE）公司的产品。GE Digital Energy MDS PulseNET是一套用于监控工业通讯网络设备的软件。MDS PulseNET Enterprise是其中的一个企业版。

GE Digital Energy MDS PulseNET和MDS PulseNET Enterprise 3.1.5之前版本的FileDownloadServlet中的下载功能中存在绝对路径遍历漏洞。远程攻击者可借助完整的路径名利用该漏洞读取或删除任意文件。

（2）CNNVD-201401-124

漏洞名称：QNAP QTS cgi-bin/jc.cgi脚本绝对路径遍历漏洞

漏洞简介：

QNAP QTS是威联通（QNAP Systems）公司的一套Turbo NAS作业系统。该系统可提供档案储存、管理、备份，多媒体应用及安全监控等功能。

QNAP QTS 4.1.0之前版本中的cgi-bin/jc.cgi脚本中存在绝对路径遍历漏洞。远程攻击者可借助‘f’参数中的完整路径名利用该漏洞读取任意文件。

（3）CNNVD-201609-650

漏洞名称：Huawei eSight 路径遍历漏洞

漏洞简介：

Huawei eSight是中国华为（Huawei）公司的一套新一代面向企业基础网络、统一通信、智真会议、视频监控和数据中心的整体运维管理解决方案。该方案支持对多厂商和多类型的设备进行统一的监控和配置管理，并对网络和业务质量进行监视和分析。

Huawei eSight V300R002C00、V300R003C10和V300R003C20版本中存在路径遍历漏洞，该漏洞源于程序没有充分验证路径。远程攻击者可利用该漏洞下载未授权文件，造成信息泄露。

**12. 后置链接（CWE-59: Link Following）**

**12.1 描述**

软件尝试使用文件名访问文件，但该软件没有正确阻止表示非预期资源的链接或者快捷方式的文件名。

**12.2 常见后果**

技术影响：Read files or directories; Modify files or directories; Bypass protection mechanism

影响范围：机密性、完整性和可用性

**12.3 与其他漏洞类型关系**

上级漏洞类型：输入验证（CWE-20）

**12.4 漏洞实例**

（1）CNNVD-201510-002

漏洞名称：Apport 后置链接漏洞

漏洞简介：

Ubuntu是英国科能（Canonical）公司和Ubuntu基金会共同开发的一套以桌面应用为主的GNU/Linux操作系统。Apport是其中的一个用于收集并反馈错误信息（当应用程序崩溃时操作系统认为有用的信息）的工具包。

Apport 2.18.1及之前的版本中的kernel_crashdump文件存在安全漏洞。本地攻击者可通过对/var/crash/vmcore.log文件实施符号链接攻击或硬链接攻击利用该漏洞造成拒绝服务（磁盘消耗）或获取权限。

（2）CNNVD-201404-248

漏洞名称：Red Hat libvirt LXC驱动程序后置链接漏洞

漏洞简介：

Red Hat libvirt是美国红帽（Red Hat）公司的一个用于实现Linux虚拟化功能的Linux API，它支持各种Hypervisor，包括Xen和KVM，以及QEMU和用于其他操作系统的一些虚拟产品。

Red Hat libvirt 1.0.1至1.2.1版本的LXC驱动程序(lxc/lxc_driver.c)中存在安全漏洞。本地攻击者可利用该漏洞借助virDomainDeviceDettach API删除任意主机设备；借助virDomainDeviceAttach API创建任意节点(mknod)；并借助virDomainShutdown或virDomainReboot API造成拒绝服务（关闭或重新启动主机操作系统）。

（3）CNNVD-201404-363

漏洞名称：Python Image Library和Pillow 后置链接漏洞

漏洞简介：

Python Image Library（PIL）是瑞士软件开发者Fredrik Lundh所研发的一个Python图像处理库。Pillow是对PIL的一些BUG修正后的编译版。

PIL 1.1.7及之前的版本和Pillow 2.3.0及之前的版本中的JpegImagePlugin.py文件的‘load_djpeg’函数；EpsImagePlugin.py文件的‘Ghostscript’函数；IptcImagePlugin.py文件的‘load’函数；Image.py文件的‘_copy’函数存在安全漏洞，该漏洞源于程序没有正确创建临时文件。本地攻击者可通过对临时文件的符号链接攻击利用该漏洞覆盖任意文件，获取敏感信息。

**13. 注入（CWE-74: Injection）**

**13.1 描述**

软件使用来自上游组件的受外部影响的输入，构造全部或部分命令、数据结构或记录，但是没有过滤或没有正确过滤掉其中的特殊元素，当发送给下游组件时，这些元素可以修改其解析或解释方式。

软件对于构成其数据和控制的内容有其特定的假设，然而，由于缺乏对用户输入的验证而导致注入问题。

**13.2 常见后果**

技术影响：Read application data; Bypass protection mechanism;  Alter execution logic; Hide activities

影响范围：机密性、完整性

**13.3 与其他漏洞类型关系**

上级漏洞类型：输入验证（CWE-20）

上级漏洞类型：格式化字符串（CWE-134）、命令注入（CWE-77）、跨站脚本（CWE-79）、代码注入（CWE-94）、SQL注入（CWE-74）

**13.4 漏洞实例**

（1）CNNVD-201505-517

漏洞名称：IBM Security SiteProtector System 安全漏洞

漏洞简介：

IBM Security SiteProtector System是美国IBM公司的一套可统一管理和分析网络、服务器和终端安全性代理及设备的集中式管理系统。

IBM Security SiteProtector System中存在安全漏洞。远程攻击者可利用该漏洞注入参数。以下版本受到影响：IBM Security SiteProtector System 3.0.0.7之前3.0版本，3.1.0.4之前3.1版本，3.1.1.2之前3.1.1版本。

（2）CNNVD-201501-611

漏洞名称：Apereo Central Authentication Service 权限许可和访问控制漏洞

漏洞简介：

Apereo Central Authentication Service（CAS）Server是Apereo基金会下的Jasig项目的一套为认证用户访问应用程序提供了可信方式的认证系统。

Apereo CAS Server 3.5.3之前版本中存在安全漏洞。远程攻击者可借助特制的用户名利用该漏洞实施LDAP注入攻击。

（3）CNNVD-201507-669

漏洞名称：Apache Groovy 代码注入漏洞

漏洞简介：

Apache Groovy是美国阿帕奇（Apache）软件基金会的一种基于JVM的敏捷开发语言，它结合了Python、Ruby和Smalltalk的许多强大的特性。

Apache Groovy 1.7.0版本至2.4.3版本的runtime/MethodClosure.java文件中的MethodClosure类存在安全漏洞。远程攻击者可借助特制的序列化

对象利用该漏洞执行任意代码，或造成拒绝服务。

**14. 代码注入（CWE-94: Code Injection）**

**14.1 描述**

软件使用来自上游组件的受外部影响的输入构造全部或部分代码段，但是没有过滤或没有正确过滤掉其中的特殊元素，这些元素可以修改发送给下游组件的预期代码段。

当软件允许用户的输入包含代码语法时，攻击者可能会通过伪造代码修改软件的内部控制流。此类修改可能导致任意代码执行。

**14.2 常见后果**

技术影响：Bypass protection mechanism; Gain privileges / assume identity; Execute unauthorized code or commands; Hide activities

影响范围：机密性、完整性和可用性

**14.3 与其他漏洞类型关系**

上级漏洞类型：注入（CWE-74）

**14.4 漏洞实例**

（1）CNNVD-201504-592

漏洞名称：Magento Community Edition和Enterprise Edition PHP远程文件包含漏洞

漏洞简介：

Magento是美国Magento公司的一套开源的PHP电子商务系统，它提供权限管理、搜索引擎和支付网关等功能。Magento Community Edition（CE）是一个社区版。Magento Enterprise Edition（EE）是一个企业版。

Magento CE 1.9.1.0版本和EE 1.14.1.0版本的Mage_Core_Block_Template_Zend类中的‘fetchView’函数存在PHP远程文件包含漏洞。远程攻击者可借助URL利用该漏洞执行任意PHP代码。

（2）CNNVD-201608-522

漏洞名称：Huawei UMA 命令注入漏洞

漏洞简介：

Huawei Unified Maintenance Audit（UMA）是中国华为（Huawei）公司的一套IT核心资源运维管理与安全审计平台。该平台通过对各种IT资源的帐号、认证、授权和审计的集中管理和控制，可满足用户IT运维管理和IT内控外审的需求。

Huawei UMA V200R001C00SPC200之前的版本中存在命令注入漏洞。远程攻击者可借助特制的字符利用该漏洞获取设备的敏感信息，或修改设备数据，造成设备失效。

（3）CNNVD-201606-609

漏洞名称：phpMyAdmin 安全漏洞

漏洞简介：

phpMyAdmin是phpMyAdmin团队开发的一套免费的、基于Web的MySQL数据库管理工具。该工具能够创建和删除数据库，创建、删除、修改数据库表，执行SQL脚本命令等。

phpMyAdmin中存在安全漏洞，该漏洞源于程序没有正确选择分隔符来避免使用preg_replace e修饰符。远程攻击者可借助特制的字符串利用该漏洞执行任意PHP代码。以下版本受到影响：phpMyAdmin 4.0.10.16之前4.0.x版本，4.4.15.7之前4.4.x版本，4.6.3之前4.6.x版本。

**15. 命令注入（CWE-77: Command Injection）**

**15.1 描述**

软件使用来自上游组件的受外部影响的输入构造全部或部分命令，但是没有过滤或没有正确过滤掉其中的特殊元素，这些元素可以修改发送给下游组件的预期命令。

命令注入漏洞通常发生在（1）输入数据来自非可信源；（2）应用程序使用输入数据构造命令；（3）通过执行命令，应用程序向攻击者提供了其不该拥有的权限或能力。

**15.2 常见后果**

技术影响：Execute unauthorized code or commands

影响范围：机密性、完整性和可用性

**15.3 与其他漏洞类型关系**

上级漏洞类型：注入（CWE-74）

下级漏洞类型：操作系统命令注入（CWE-78）

**15.4 漏洞实例**

（1）CNNVD-201504-057

漏洞名称：Apache Cassandra 操作系统命令注入漏洞

漏洞简介：

Apache Cassandra是美国阿帕奇（Apache）软件基金会的一套开源分布式NoSQL数据库系统。

Apache Cassandra的默认配置中存在安全漏洞，该漏洞源于程序对所有JMX的网络接口绑定了未经身份验证的RMI接口。远程攻击者可通过发送RMI请求利用该漏洞执行任意Java代码。以下版本受到影响：Apache Cassandra 1.2.0版本至1.2.19版本，2.0.0版本至2.0.13版本，2.1.0版本至2.1.3版本。

（2）CNNVD-201503-063

漏洞名称：Common LaTeX Service Interface 代码注入漏洞

漏洞简介：

ShareLaTeX是ShareLaTeX团队开发的一款开源的基于Web的实时协作LaTex编辑器，它支持本地编辑、实时协作和编译LaTeX文档。Common LaTeX Service Interface（CLSI）是一个提供了编译LaTeX文档的API的通用LaTeX服务接口。

ShareLaTeX 0.1.3之前版本中使用的CLSI 0.1.3之前版本中存在安全漏洞。远程攻击者可借助文件名中的‘`’（反引号）字符利用该漏洞执行任意代码。

（3）CNNVD-201507-077

漏洞名称：Apple OS X Spotlight组件任意命令执行漏洞

漏洞简介：

Apple OS X是美国苹果（Apple）公司为Mac计算机所开发的一套专用操作系统。Spotlight是其中的一个能够在输入框内快速检索整个系统（包含文件、邮件和联系方式等）的组件。

Apple OS X 10.10.4之前版本的Spotlight组件中存在安全漏洞。攻击者可借助本地照片库中特制的照片文件名称利用该漏洞执行任意命令。

**16. SQL注入（CWE-89: SQL Injection）**

**16.1 描述**

软件使用来自上游组件的受外部影响的输入构造全部或部分SQL命令，但是没有过滤或没有正确过滤掉其中的特殊元素，这些元素可以修改发送给下游组件的预期SQL命令。

如果在用户可控输入中没有充分删除或引用SQL语法，生成的SQL查询可能会导致这些输入被解释为SQL命令而不是普通用户数据。利用SQL注入可以修改查询逻辑以绕过安全检查，或者插入修改后端数据库的其他语句，如执行系统命令。

**16.2 常见后果**

技术影响：Read application data; Modify application data; Bypass protection mechanism

影响范围：机密性、完整性

**16.3 与其他漏洞类型关系**

上级漏洞类型：注入（CWE-74）

**16.4 漏洞实例**

（1）CNNVD-201610-761

漏洞名称：Cisco Identity Services Engine SQL注入漏洞

漏洞简介：

Cisco Identity Services Engine（ISE）Software是美国思科（Cisco）公司的一款基于身份的环境感知平台（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 ISE Software 1.3(0.876)版本中的Web框架代码中存在SQL注入漏洞。远程攻击者可通过发送恶意的URL利用该漏洞在数据库中执行任意SQL命令。

（2）CNNVD-201505-543

漏洞名称：OSIsoft PI AF和PI SQL for AF 安全漏洞

漏洞简介：

OSIsoft PI AF（Asset Framework）是美国OSIsoft公司的一套可为资产定义一致的呈现方式并提供结构化信息的资产框架，它支持将资产属性与关系数据库进行关联、基于资产的数据分析和应用计算等。PI SQL for AF是其中的一个SQL访问接口。

OSIsoft PI AF 2.6版本和2.7版本和PI SQL for AF 2.1.2.19版本中存在安全漏洞，该漏洞源于程序向PI SQL(AF)Trusted Users组插入Everyone账户。远程攻击者可借助SQL语句利用该漏洞绕过既定的命令限制。

（3）CNNVD-201606-011

漏洞名称：Apache Ranger SQL注入漏洞

漏洞简介：

Apache Ranger是美国阿帕奇（Apache）软件基金会的一套为Hadoop集群实现全面安全措施的架构，它针对授权、结算和数据保护等核心企业安全要求，提供中央安全政策管理。

Apache Ranger 0.5.3之前0.5.x版本的策略管理工具中存在SQL注入漏洞。远程攻击者可借助service/plugins/policies/eventTime URI的‘eventTime’参数利用该漏洞执行任意SQL命令。

**17. 操作系统命令注入（CWE-78: OS Command Injection）**

**17.1 描述**

软件使用来自上游组件的受外部影响的输入构造全部或部分操作系统命令，但是没有过滤或没有正确过滤掉其中的特殊元素，这些元素可以修改发送给下游组件的预期操作系统命令。

此类漏洞允许攻击者在操作系统上直接执行意外的危险命令。

**17.2 常见后果**

技术影响：Execute unauthorized code or commands; DoS: crash / exit / restart; Read files or directories; Modify files or directories; Read application data; Modify application data; Hide activities

影响范围：机密性、完整性和可用性

**17.3 与其他漏洞类型关系**

上级漏洞类型：命令注入（CWE-77）

**17.4 漏洞实例**

（1）CNNVD-201610-689

漏洞名称：IBM Security Guardium Database Activity Monitor 操作系统命令注入漏洞

漏洞简介：

IBM Security Guardium Database Activity Monitor是美国IBM公司的一款数据库活动监控器产品。该产品提供合规性自动化控制和防止内外部威胁等功能。

IBM Security Guardium Database Activity Monitor中存在操作系统命令注入漏洞。攻击者可借助检索字段利用该漏洞以root权限执行任意命令。以下版本受到影响：IBM Security Guardium Database Activity Monitor 8.2，9.0，9.1，9.5，10.0，10.0.1，10.1。

（2）CNNVD-201609-503

漏洞名称：Cisco Cloud Services Platform 命令注入漏洞

漏洞简介：

Cisco Cloud Services Platform（CSP）是美国思科（Cisco）公司的一套用于数据中心网络功能虚拟化的软硬件平台。web-based GUI是其中的一个基于Web的图形用户界面组件。

Cisco CSP 2100 2.0版本中的web-based GUI存在命令注入漏洞。远程攻击者可借助特制的平台命令利用该漏洞以root权限执行任意操作系统命令。

（3）CNNVD-201509-254

漏洞名称：Symantec Web Gateway 操作系统命令注入漏洞

漏洞简介：

Symantec Web Gateway（SWG）是美国赛门铁克（Symantec）公司的一套网络内容过滤软件。该软件提供网络内容过滤、数据泄露防护等功能。

使用5.2.2 DB 5.0.0.1277之前版本软件的SWG设备中的管理控制台中存在安全漏洞。远程攻击者可借助‘redirect.’字符串利用该漏洞绕过既定的访问限制，执行任意命令。

**18. 安全特征问题（CWE-254: Security Features）**

**18.1 描述**

此类漏洞是指与身份验证、访问控制、机密性、密码学、权限管理等有关的漏洞，是一些与软件安全有关的漏洞。如果有足够的信息，此类漏洞可进一步分为更低级别的类型。

**18.2 与其他漏洞类型关系**

上级漏洞类型：代码问题（CWE-17）

下级漏洞类型：授权问题（CWE-287）、未充分验证数据可靠性（CWE-345）、信任管理（CWE-255）、权限许可和访问控制（CWE-264）、加密问题（CWE-310）

**18.3 漏洞实例**

（1）CNNVD-201502-438

漏洞名称：Mozilla Firefox 安全漏洞

漏洞简介：

Mozilla Firefox是美国Mozilla基金会开发的一款开源Web浏览器。

Mozilla Firefox 35.0.1及之前版本中存在安全漏洞，该漏洞源于程序没有正确识别末尾附加‘.’字符的域名。攻击者可通过构建带有‘.’字符的URL，并访问该域的X.509证书利用该漏洞实施中间人攻击，绕过HPKP和HSTS保护机制。

（2）CNNVD-201504-054

漏洞名称：Inductive Automation Ignition 安全漏洞

漏洞简介：

Inductive Automation Ignition是美国Inductive Automation公司的一套人机界面（HMI）/SCADA系统，它是FactoryPMI的更新版本。

Inductive Automation Ignition 7.7.2版本中存在安全漏洞，该漏洞源于程序在用户执行注销操作后没有终止会话。远程攻击者可利用该漏洞绕过既定的访问限制。

（3）CNNVD-201506-579

漏洞名称：Google Chrome Blink 安全漏洞

漏洞简介：

Google Chrome是美国谷歌（Google）公司开发的一款Web浏览器。Blink是美国谷歌（Google）公司和挪威欧朋（Opera Software）公司共同开发的一套浏览器排版引擎（渲染引擎）。

Google Chrome 43.0.2357.81及之前版本中使用的Blink中的bindings/scripts/v8_types.py文件存在安全漏洞，该漏洞源于程序没有正确为返回值的DOM封装器选择创建环境。远程攻击者可借助特制的JavaScript代码利用该漏洞绕过同源策略。

**19. 授权问题（CWE-287: Improper Authentication）**

**19.1 描述**

程序没有进行身份验证或身份验证不足，此类漏洞是与身份验证有关的漏洞。

**19.2 常见后果**

技术影响：Read application data; Gain privileges / assume identity; Execute unauthorized code or commands

影响范围：机密性、完整性和可用性

**19.3 与其他漏洞类型关系**

上级漏洞类型：安全特征问题（CWE-254）

**19.4 漏洞实例**

（1）CNNVD-201609-629

漏洞名称：Microsoft Passport-Azure-AD for Node.js库安全漏洞

漏洞简介：

Microsoft Azure Active Directory Passport（又名Passport-Azure-AD）library for Node.js是美国微软（Microsoft）公司的一个使用了Node.js（网络应用平台）的Passport策略库（集合），它用于帮助将节点应用程序与Windows Azure Active Directory（提供了云端的身份和访问管理的服务）集成，包括OpenID Connect、WS-Federation和SAML-P身份验证和授权等程序。

Microsoft Azure Active Directory Passport for Node.js库中存在安全漏洞。远程攻击者可借助特制的令牌利用该漏洞绕过Azure Active Directory身份验证。以下版本受到影响：Microsoft Azure Active Directory Passport library 1.4.6之前的1.x版本和2.0.1之前的2.x 版本。

（2）CNNVD-201602-365

漏洞名称：Apache Ranger 身份验证绕过漏洞

漏洞简介：

Apache Ranger是美国阿帕奇（Apache）软件基金会的一套为Hadoop集群实现全面安全措施的架构，它针对授权、结算和数据保护等核心企业安全要求，提供中央安全政策管理。

Apache Ranger 0.5.1之前版本的Admin UI中存在安全漏洞，该漏洞源于程序没有正确处理缺少密码的身份验证请求。远程攻击者可借助已知的有效用户名利用该漏洞绕过身份验证机制。

（3）CNNVD-201511-421

漏洞名称：Moxa OnCell Central Manager Software 授权问题漏洞

漏洞简介：

Moxa OnCell Central Manager是摩莎（Moxa）公司的一套私有IP管理软件。该软件支持在网络上通过专用网络来配置、管理和监控远程设备等。

Moxa OnCell Central Manager 2.0及之前版本的MessageBrokerServlet servlet中存在安全漏洞，该漏洞源于程序没有要求执行身份验证。远程攻击者可借助命令利用该漏洞获取管理员访问权限。

**20. 信任管理（CWE-255: Credentials Management）**

**20.1 描述**

此类漏洞是与证书管理相关的漏洞。包含此类漏洞的组件通常存在默认密码或者硬编码密码、硬编码证书。

**20.2 与其他漏洞类型关系**

上级漏洞类型：安全特征问题（CWE-254）

**20.3 漏洞实例**

（1）CNNVD-201608-007

漏洞名称：Crestron Electronics DM-TXRX-100-STR 安全漏洞

漏洞简介：

Crestron Electronics DM-TXRX-100-STR是美国Crestron Electronics公司的一款流编码器/解码器产品。

使用1.3039.00040及之前版本固件的Crestron Electronics DM-TXRX-100-STR设备存在安全漏洞，该漏洞源于管理员账户存在硬编码密码。远程攻击者可通过Web管理界面利用该漏洞获取权限。

（2）CNNVD-201501-375

漏洞名称：Ceragon FiberAir IP-10 安全漏洞

漏洞简介：

Ceragon FiberAir IP-10是以色列Ceragon公司的一款无线微波传输设备。

Ceragon FiberAir IP-10网桥中存在安全漏洞，该漏洞源于root账户使用默认的密码。远程攻击者可借助HTTP、SSH、TELNET或CLI会话利用该漏洞获取访问权限。

（3）CNNVD-201601-663

漏洞名称：phpMyAdmin 安全漏洞

漏洞简介：

phpMyAdmin是phpMyAdmin团队开发的一套免费的、基于Web的MySQL数据库管理工具。该工具能够创建和删除数据库，创建、删除、修改数据库表，执行SQL脚本命令等。

phpMyAdmin的js/functions.js文件中的‘suggestPassword’函数存在安全漏洞，该漏洞源于程序使用的Math.random JavaScript函数没有提供安全的随机数。远程攻击者可通过实施暴力破解攻击利用该漏洞猜出密码。以下版本受到影响：phpMyAdmin 4.0.10.13之前4.0.x版本，4.4.15.3之前4.4.x版本，4.5.4之前4.5.x版本。

**21. 加密问题（CWE-310: Cryptographic Issues）**

**21.1 描述**

此类漏洞是与加密使用有关的漏洞，涉及内容加密、密码算法、弱加密（弱口令）、明文存储敏感信息等。

**21.2 与其他漏洞类型关系**

上级漏洞类型：安全特征问题（CWE-254）

**21.3 漏洞实例**

（1）CNNVD-201610-012

漏洞名称：Auto-Matrix Aspect-Nexus和Aspect-Matrix Building Automation Front-End Solutions 安全漏洞

漏洞简介：

Auto-Matrix Aspect-Nexus和Aspect-Matrix Building Automation Front-End Solutions都是美国Auto-Matrix公司的用于基础设施的建筑自动化前端解决方案，该方案主要在美国本土的商业设施、关键制造、能源和污水系统等领域（工控）进行部署。

Auto-Matrix Aspect-Nexus Building Automation Front-End Solutions应用程序3.0.0之前的版本和Aspect-Matrix Building Automation Front-End Solutions应用程序中存在安全漏洞，该漏洞源于程序以明文方式存储密码。远程攻击者可通过读取文件利用该漏洞获取敏感信息。

（2）CNNVD-201609-487

漏洞名称：Apple OS X Server ServerDocs Server 安全漏洞

漏洞简介：

Apple OS X Server是美国苹果（Apple）公司的一套基于Unix的服务器操作软件。该软件可实现文件共享、会议安排、网站托管、网络远程访问等。ServerDocs Server是其中的一个服务组件。

Apple OS X Server 5.2之前的版本支持RC4加密算法中的ServerDocs Server存在安全漏洞。远程攻击者可利用该漏洞破解密码保护机制。

（3）CNNVD-201605-118

漏洞名称：OpenSSL 安全漏洞

漏洞简介：

OpenSSL是OpenSSL团队开发的一个开源的能够实现安全套接层（SSL v2/v3）和安全传输层（TLS v1）协议的通用加密库，它支持多种加

密算法，包括对称密码、哈希算法、安全散列算法等。

OpenSSL 0.9.6之前版本的crypto/rsa/rsa_gen.c文件中存在安全漏洞，该漏洞源于程序没有正确处理超过表达式大小的C bitwise-shift操作。远程攻击者可借助64-bit HP-UX平台上不正确的RSA密钥生成，利用该漏洞破坏加密保护机制。

**22. 未充分验证数据可靠性（CWE-345: Insufficient Verification of Data Authenticity）**

**22.1 描述**

程序没有充分验证数据的来源或真实性，导致接受无效的数据。

**22.2 常见后果**

技术影响：Varies by context; Unexpected state

影响范围：完整性

**22.3 与其他漏洞类型关系**

上级漏洞类型：安全特征问题（CWE-254）

下级漏洞类型：跨站请求伪造（CWE-352）

**22.4 漏洞实例**

（1）CNNVD-201504-100

漏洞名称：Subversion mod_dav_svn服务器安全漏洞

漏洞简介：

Apache Subversion是美国阿帕奇（Apache）软件基金会的一套开源的版本控制系统，该系统可兼容并发版本系统(CVS)。

Subversion 1.5.0版本至1.7.19版本和1.8.0版本至1.8.11版本的mod_dav_svn服务器中存在安全漏洞。远程攻击者可通过发送特制的v1 HTTP协议请求序列利用该漏洞伪造svn:author属性。

（2）CNNVD-201504-018

漏洞名称：OpenStack Compute 安全漏洞

漏洞简介：

OpenStack是美国国家航空航天局（National Aeronautics and Space Administration）和美国Rackspace公司合作研发的一个云平台管理项目。OpenStack Compute（Nova）是其中的一个使用Python语言编写的云计算构造控制器，属于IaaS系统的一部分。

OpenStack Compute中存在安全漏洞，该漏洞源于程序没有验证websocket请求的源。远程攻击者可借助特制的网页利用该漏洞访问控制台。以下版本受到影响：OpenStack Compute 2014.1.3及之前版本，2014.2.1版本，2014.2.2版本。

（3）CNNVD-201603-369

漏洞名称：CA Single Sign-On non-Domino Web代理安全漏洞

CA Single Sign-On（又名SSO，前称SiteMinder）是美国CA公司的一套通过单点登录安全访问Web应用程序的软件。

CA Single Sign-On的non-Domino Web代理中存在安全漏洞。远程攻击者可通过发送特制的请求利用该漏洞造成拒绝服务（守护进程崩溃），或获取敏感信息。以下版本受到影响：CA Single Sign-On R6版本，SP3 CR13之前R12.0版本，SP3 CR1.2之前R12.0J版本，CR5之前R12.5版本。

**23. 跨站请求伪造（CWE-352: Cross-Site Request Forgery）**

**23.1 描述**

Web应用程序没有或不能充分验证有效的请求是否来自可信用户。

如果web服务器不能验证接收的请求是否是客户端特意提交的，则攻击者可以欺骗客户端向服务器发送非预期的请求，web服务器会将其视为真实请求。这类攻击可以通过URL、图像加载、XMLHttpRequest等实现，可能导致数据暴露或意外的代码执行。

**23.2 常见后果**

技术影响：Gain privileges / assume identity; Bypass protection mechanism; Read application data; Modify application data; DoS: crash / exit / restart

影响范围：机密性、完整性和可用性

**23.3 与其他漏洞类型关系**

上级漏洞类型：未充分验证数据可靠性（CWE-345）

**23.4 漏洞实例**

（1）CNNVD-201610-744

漏洞名称：Yandex Browser for desktop 跨站请求伪造漏洞

漏洞简介：

Yandex Browser for desktop是俄罗斯Yandex公司的一款桌面版浏览器。

Yandex Browser for desktop 16.6之前的版本中的synchronization form存在跨站请求伪造漏洞。远程攻击者可利用该漏洞窃取浏览器配置文件中存储的数据，执行未授权操作。

（2）CNNVD-201609-619

漏洞名称：Django 跨站请求伪造漏洞

漏洞简介：

Django是Django软件基金会的一套基于Python语言的开源Web应用框架。该框架包括面向对象的映射器、视图系统、模板系统等。

Django 1.8.15之前的版本和1.9.10之前的1.9.x版本中的cookie解析代码存在跨站请求伪造漏洞。远程攻击者可通过设置任意cookie利用该漏洞绕过既定的CSRF保护机制。

（3）CNNVD-201609-125

漏洞名称：Huawei WS331a 跨站请求伪造漏洞

漏洞简介：

Huawei WS331a是中国华为（Huawei）公司的一款迷你无线路由器。

使用WS331a-10 V100R001C01B112之前版本软件的Huawei WS331a路由器的管理界面存在跨站请求伪造漏洞。远程攻击者可通过提交特制的请求利用该漏洞恢复出厂设置或重启设备。

**24. 权限许可和访问控制（CWE-264: Permissions, Privileges, and Access Controls）**

**24.1 描述**

此类漏洞是与许可、权限和其他用于执行访问控制的安全特征的管理有关的漏洞。

**24.2 与其他漏洞类型关系**

上级漏洞类型：安全特征问题（CWE-254）

下级漏洞类型：访问控制错误（CWE-284）

**24.3 漏洞实例**

（1）CNNVD-201609-661

漏洞名称：Drupal 安全漏洞

漏洞简介：

Drupal是Drupal社区所维护的一套用PHP语言开发的免费、开源的内容管理系统。

Drupal 8.1.10之前的8.x版本中存在安全漏洞，该漏洞源于程序没有正确检查‘Administer comments’权限。远程攻击者可借利用该漏洞设置任意节点的评论可见。

（2）CNNVD-201610-281

漏洞名称：Microsoft Windows 诊断中心特权提升漏洞

漏洞简介：

Microsoft Windows是美国微软（Microsoft）公司发布的一系列操作系统。

Microsoft Windows中的Standard Collector Service存在特权提升漏洞，该漏洞源于程序没有正确处理库加载。本地攻击者可借助特制的应用程序利用该漏洞以提升的权限执行任意代码。以下产品和版本受到影响：Microsoft Windows 10 Gold，1511，1607。

（3）CNNVD-201610-226

漏洞名称：Android Synaptics触屏驱动程序安全漏洞

漏洞简介：

Android on Nexus 5X是美国谷歌（Google）公司和开放手持设备联盟（简称OHA）共同开发的一套运行于Nexus 5X（智能手机）中并以Linux为基础的开源操作系统。Synaptics touchscreen driver是用于其中的一个Synaptics触屏驱动。

基于Nexus 5X设备上的Android 2016-10-05之前的版本中的Synaptics触屏驱动程序存在安全漏洞。攻击者可借助特制的应用程序利用该漏洞获取权限。

**25. 访问控制错误（CWE-284: Improper Access Control）**

**25.1 描述**

软件没有或者没有正确限制来自未授权角色的资源访问。

访问控制涉及若干保护机制，例如认证（提供身份证明）、授权（确保特定的角色可以访问资源）与记录（跟踪执行的活动）。当未使用保护机制或保护机制失效时，攻击者可以通过获得权限、读取敏感信息、执行命令、规避检测等来危及软件的安全性。

**25.2 常见后果**

技术影响：Varies by context

**25.3 与其他漏洞类型关系**

上级漏洞类型：权限许可和访问控制（CWE-264）

**25.4 漏洞实例**

（1）CNNVD-201504-462

漏洞名称：Red Hat PicketLink Service Provider组件安全漏洞

漏洞简介：

Red Hat PicketLink是美国红帽（Red Hat）公司的一套用于Java应用程序的统一身份管理框架。

Red Hat PicketLink 2.7.0之前版本的Service Provider(SP)组件中存在安全漏洞，该漏洞源于程序没有正确考虑SAML断言的Audience条件。远程攻击者可利用该漏洞登录其他用户账户。

（2）CNNVD-201505-027

漏洞名称：EMC SourceOne Email Management 安全漏洞

漏洞简介：

EMC SourceOne Email Management是美国易安信（EMC）公司的一套电子邮件归档软件。该软件提供邮件生命周期管理、邮件捕获和邮件搜索等功能。

EMC SourceOne Email Management 7.1及之前版本中存在安全漏洞，该漏洞源于程序没有为无效的登录尝试次数设置锁机制。远程攻击者可通过实施暴力破解攻击利用该漏洞获取访问权限。

（3）CNNVD-201502-450

漏洞名称：Mozilla Firefox 安全绕过漏洞

漏洞简介：

Mozilla Firefox是美国Mozilla基金会开发的一款开源Web浏览器。

Mozilla Firefox 35.0.1及之前版本中存在安全漏洞，该漏洞源于程序没有正确限制JavaScript对象从non-extensible状态到extensible状态的转换。远程攻击者可借助特制的Web网站利用该漏洞绕过Caja Compiler或Secure EcmaScript沙箱保护机制。

**26. 资料不足**

**26.1 描述**

根据目前信息暂时无法将该漏洞归入上述任何类型，或者没有足够充分的信息对其进行分类，漏洞细节未指明。

**26.2 漏洞实例**

（1）CNNVD-201611-132

漏洞名称：Adobe Flash Player 类型混淆漏洞

漏洞简介：

Adobe Flash Player是美国奥多比（Adobe）公司的一款跨平台、基于浏览器的多媒体播放器产品。该产品支持跨屏幕和浏览器查看应用程序、内容和视频。

Adobe Flash Player 23.0.0.205及之前的版本和11.2.202.643及之前的版本中存在类型混淆漏洞。攻击者可利用该漏洞执行任意代码。

（2）CNNVD-201605-521

漏洞名称：Apple OS X El Capitan IOAcceleratorFamily 任意代码执行漏洞

漏洞简介：

Apple OS X El Capitan是美国苹果（Apple）公司为Mac计算机所开发的一套专用操作系统。

Apple OS X El Capitan 10.11.5之前版本的IOAcceleratorFamily中存在安全漏洞。攻击者可借助特制的应用利用该漏洞以内核权限执行任意代码或造成拒绝服务（空指针逆向引用）。

（3）CNNVD-201606-343

漏洞名称：Adobe Flash Player 安全漏洞

漏洞简介：

Adobe Flash Player是美国奥多比（Adobe）公司的一款跨平台、基于浏览器的多媒体播放器产品。该产品支持跨屏幕和浏览器查看应用程序、内容和视频。

基于Windows、Macintosh、Linux和Chrome OS平台的Adobe Flash Player 21.0.0.242及之前版本中存在安全漏洞。远程攻击者可利用该漏洞执行任意代码，控制受影响系统。

## 四、漏洞类型的判别过程

本指南中漏洞类型具有层次关系，在判别漏洞类型时可根据漏洞类型的层次树，自左向右依次进行判断。

具体过程如下：当进行到某节点时，（1）如果该节点为叶子节点，判断结束，漏洞类型为当前节点的类型；（2）否则该节点为中间节点，并且①根据漏洞信息无法进一步判断该漏洞属于当前节点的哪个子类型时，则漏洞类型为当前节点的类型；②否则，选择子类型节点，继续（1）和（2）。