医疗器械网络安全漏洞自评报告

报告名称：外部软件环境评估报告

报告机构：中国信息安全测评中心

提 供 方： 国家信息安全漏洞库

目录

1. 目的

医疗器械网络安全注册审查指导原则（2022 年修订版）明确规定了漏洞评估的要求：根据医疗器械网络安全注册审查指导原则（2022 年修订版）的要求，我们建议包括 CVSS 漏洞等级、漏洞扫描报告、漏洞总数和剩余漏洞数、剩余漏洞的维护方案等内容。

对于轻微级别，需要提供依据 CVSS 的漏洞等级和漏洞数，而对于中等和严重级别，需要提供网络安全漏洞自评报告。

2. 引用文件

参考资料：

编制医疗器械网络安全漏洞自评报告要点解析

国家信息安全漏洞库

Debian 安全信息

国家计算机网络入侵防范中心

360 安全周报

3. CVSS 漏洞等级

3.1 概述

CNNVD 漏洞编码规范

3.1.1 适用范围说明

凡是被 CNNVD 漏洞库收录的漏洞，均适用此编码语法规范,包括采集的公开漏洞以及收录的未公开漏洞。

3.1.2 CNNVD-ID 定义

CNNVD 漏洞库收录漏洞数据后，为便于识别且体现数据唯一性、规范性、兼容性，统一为每一条漏洞分配一个唯一的编号，即 CNNVD-ID。

3.1.3 编码原则

1)唯一性：每条漏洞数据的编号是唯一的。

2)易识别性：易于识别数据产生的时间。

3)透明性：编码中避免暴露业务信息。

3.1.4 CNNVD-ID 语法介绍

CNNVD + 年、月 + 任意数字

其中，“CNNVD”为固定编码前缀；“年”为四位；“月”为两位；“任意数字”从固定的三位开始，在有需要的时候扩展位数。举例：

固定三位ID	当需要4位ID时	当需要5位ID时
CNNVD-201501-001	CNNVD-201501-1001	CNNVD-201501-10001
°	°	°
°	°	°
°	°	°
CNNVD-201501-999	CNNVD-201501-9999	CNNVD-201501-99999

3.2 指标分析

CNNVD 漏洞分级规范

3.2.1 基本指标

本标准使用两组指标对漏洞进行评分，分别是可利用性指标组和影响性指标组。可利用性指标组描述漏洞利用的方式和难易程度，反映脆弱性组件的特征，应依据脆弱性组件进行评分，影响性指标组描述漏洞被成功利用后给受影响组件造成的危害，应依据受影响组件进行评分。

3.2.1.1 可用性指标

可利用性指标组刻画脆弱性组件（即包含漏洞的事物）的特征，反映漏洞利用的难易程度和技术要求等。可利用性指标组包含四个指标，分别是攻击途径、攻击复杂度、权限要求和用户交互。每一个指标的取值都应当根据脆弱性组件进行判断，并且在判断某个指标的取值时不考虑其他指标。

1)攻击向量

该指标反映攻击者利用漏洞的途径，指是否可通过网络、邻接、本地和物理接触等方式进行利用。

攻击途径的赋值如下：

（1）网络：脆弱性组件是网络应用，攻击者可以通过互联网利用该漏洞。这类漏洞通常称为“可远程利用的”，攻击者可通过一个或多个网络跳跃（跨路由器）利用该漏洞。

（2）邻接：脆弱性组件是网络应用，但攻击者不能通过互联网（即不能跨路由器）利用该漏洞，只能在共享的物理（如，蓝牙、IEEE 802.11）或逻辑（如，本地 IP 子网）网络内利用该漏洞。

（3）本地：脆弱性组件不是网络应用，攻击者通过读/写操作或运行应用程序/工具来利用该漏洞。有时，攻击者需要本地登录，或者需要用户执行恶意文件才可利用该漏洞。当漏洞利用时需要用户去下载或接受恶意内容（或者需要本地传递恶意内容）时，攻击途径取值为“本地”。

（4）物理：攻击者必须物理接触/操作脆弱性组件才能发起攻击。物理交互可以是短暂的也可以是持续的。

例 3 假设攻击者以普通用户身份远程登录一台主机，然后在该主机上打开包含恶意内容的 PDF 文件，使得攻击者获得管理员权限。对于这种情况，攻击途径的取值是“本地”。这里不需要考虑这个恶意文件的获取方式，即使是攻击者通过网络下载到这台机器上的，攻击途径也是“本地”。

2)攻击复杂性

该指标反映攻击者利用该漏洞实施攻击的复杂程度，描述攻击者利用漏洞时是否必须存在一些超出攻击者控制能力的软件、硬件或网络条件，如软件竞争条件、应用配置等。对于必须存在特定条件才能利用的漏洞，攻击者可能需要收集关于目标的更多信息。在评估该指标时，不考虑用户交互的任何要求。

攻击复杂度的赋值如下：

（1）低：不存在专门的访问条件，攻击者可以期望重复利用漏洞。

（2）高：漏洞的成功利用依赖于某些攻击者不能控制的条件。即，攻击者不能任意发动攻击，在预期成功发动攻击前，攻击者需要对脆弱性组件投入一定数量的准备工作。包括如下一些情况：

攻击者必须对目标执行有针对性的调查。例如，目标配置的设置、序列数、共享秘密等。

攻击者必须准备目标环境以提高漏洞利用的可靠性。例如，重复利用以赢得竞争条件，或克服高级漏洞利用缓解技术。

攻击者必须将自己注入到攻击目标和受害者所请求的资源之间的逻辑网络路径中，以便读取和/或修改网络通信（如，中间人攻击）。

在攻击复杂度取值为“高”的描述中，对攻击者在成功发动攻击前所做的准备工作没有进行定量的描述，只要攻击者必须进行一些额外的努力才能利用这个漏洞，攻击复杂度就是“高”，如漏洞利用时需要配置其他的特殊状态，需要监视或者改变受攻击实体的运行状态等。如果漏洞利用时所需要的条件要求不高，例如只需构造一些简单的数据包，则攻击复杂度为“低”。

3)所需权限

该指标反映攻击者成功利用漏洞需要具备的权限层级，即利用漏洞时是否需要拥有对该组件操作的权限（如管理员权限、guest 权限）。

权限要求的赋值如下：

（1）无：攻击者在发动攻击前不需要授权，执行攻击时不需要访问任何设置或文件。

（2）低：攻击者需要取得普通用户权限，该类权限对脆弱性组件有一定的控制能力，具有部分（非全部）功能的使用或管理权限，通常需要口令等方式进行身份认证，例如，操作系统的普通用户权限、Web 等应用的注册用户权限。

（3）高：攻击者需要取得对脆弱性组件的完全控制权限。通常，该类权限对于脆弱性组件具有绝对的控制能力，例如，操作系统的管理员权限，Web 等应用的后台管理权限。

例 4 正常情况下，具有普通用户权限只能对该用户拥有的设置和文件进行操作。假设具有普通用户权限的攻击者通过利用漏洞获得权限提升，能够在目标系统上执行任意命令。对于这种情况，权限要求为“低”，至于权限提升后造成的危害，会在影响性指标组中体现。

表 1 给出了不同操作系统中权限要求的评分参考。

操作系统	权限要求	用户名/组名
Windows	高	管理员组（Administrators）
		系统组（SYSTEM）
	低	高级用户组（Power Users）
		普通用户组（Users）
		设置密码的来宾组（Guests）
	无	未设置密码的来宾组（Guests）
		匿名（ANONYMOUS）
Linux	高	系统管理员（root）
	低	系统用户（mail、halt等）
		自定义用户
	无	客人用户（guest）
macOS	高	超级用户（root）
		管理员
	低	普通成员
	无	客人用户（guest）
Android	高	开发者（root）
	低	使用者（非Root机主用户）
		访客（针对Android 4.2系统后多用户模式）
	无	暂无
iOS	高	最高权限（root 针对越狱用户）
	低	普通用户（非越狱机主用户）
		客人用户（针对启用访问限制的用户）
	无	暂无

注:本地登录的用户和远程登录的用户都可参照上述表格。

4)用户交互

该指标反映成功利用漏洞是否需要用户（而不是攻击者）的参与，该指标识别攻击者是否可以根据其意愿单独利用漏洞，或者要求其他用户以某种方式参与。

用户交互的赋值如下：

（1）不需要：无需任何用户交互即可利用漏洞。

（2）需要：漏洞的成功利用需要其他用户在漏洞被利用之前执行一些操作（打开某个文件、点击某个链接、访问特定的网页等）。

例 5 假设某个漏洞只能在系统管理员安装应用程序期间才可能被利用。对于这种情况，用户交互是“需要”。

3.2.1.2 范围

一、适用范围说明

本标准规定了信息安全漏洞危害程度的评价指标和等级划分方法。凡是被国家信息安全漏洞库（CNNVD）收录的漏洞，均适用此分级规范，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、术语和定义

（一）漏洞（vulnerability）

漏洞是计算机信息系统在需求、设计、实现、配置、运行等过程中，有意或无意产生的缺陷。这些缺陷以不同的形式存在于计算机信息系统的各个层次和环节之中，一旦被恶意主体所利用，就会对计算机信息系统的安全造成损害，从而影响计算机信息系统的正常运行。

（二）脆弱性组件（vulnerable component）

脆弱性组件指包含漏洞的组件，通常是软件应用、软件模块、驱动、甚至硬件设备等。攻击者通过利用脆弱性组件中的漏洞来发动攻击。

（三）受影响组件（impacted component）

受影响组件指漏洞被成功利用后遭受危害的组件，如软件应用、硬件设备、网络资源等。受影响组件可以是脆弱性组件本身，可以是其他软件、硬件或网络组件。

（四）影响范围（impacted scope）

影响范围指漏洞被成功利用后遭受危害的资源的范围。若受漏洞影响的资源超出了脆弱性组件的范围，则受影响组件和脆弱性组件不同；若受漏洞影响的资源局限于脆弱性组件内部，则受影响组件和脆弱性组件相同。

若受影响组件和脆弱性组件不同，则影响范围发生变化；否则，影响范围不变。本标准不仅可以度量脆弱性组件和受影响组件相同的漏洞，而且还可以度量脆弱性组件和受影响组件不同的漏洞。

例 1 假设某即时聊天工具中存在一个漏洞，攻击者利用该漏洞可造成主机系统中的部分信息（如用户的 Word 文档、管理员密码、系统配置）泄露。这个例子中，脆弱性组件是即时聊天工具，受影响组件是主机系统，脆弱性组件和受影响组件不同，漏洞的影响范围发生变化。

例 2 假设某数据库管理系统中存在一个漏洞，攻击者利用该漏洞可窃取数据库中的全部数据。这个例子中，脆弱性组件是数据库管理系统，受影响组件还是数据库管理系统，脆弱性组件和受影响组件为相同组件，漏洞的影响范围不变。

3.2.1.3 影响指标

影响性指标组反映漏洞成功利用后所带来的危害。漏洞的成功利用可能危害一个或多个组件，影响性指标组的分值应当根据遭受最大危害的组件进行评定。

影响性指标组包括三个指标，分别是机密性影响、完整性影响和可用性影响。

1)保密性

这个指标度量漏洞的成功利用对信息资源的机密性的影响。机密性指只有授权用户才能访问受保护的信息资源，限制向未授权用户披露受保护信息。机密性影响是指对受影响服务所使用的数据的影响，例如，系统文件丢失、信息暴露等。

机密性影响的赋值如下：

（1）高：机密性完全丢失，导致受影响组件的所有资源暴露给攻击者。或者，攻击者只能得到一些受限信息，但是，暴露的信息可以导致一个直接的、严重的信息丢失。例如，攻击者获得了管理员密码、Web 服务器的私有加密密钥等。

（2）低：机密性部分丢失。攻击者可以获取一些受限信息，但是攻击者不能控制获得信息的数量和种类。披露的信息不会引起受影响组件直接的、严重的信息丢失。

（3）无：受影响组件的机密性没有丢失，攻击者不能获得任何机密信息。

机密性影响为“高”表示攻击者能够获得受影响组件的全部信息，或者攻击者能够获得他想要的任何信息。或者，利用得到的部分信息能够进一步获得他想要的任何信息。

机密性影响为“低”表示攻击者只能获得部分受限信息，不能任意获取信息。利用得到的部分信息也不能进一步获得任意信息。

2)完整性

这个指标度量漏洞的成功利用给完整性造成的影响。完整性指信息的可信性与真实性，如果攻击者能够修改被攻击对象中的文件，则完整性受到影响。完整性是指对受影响服务所使用的数据的影响。例如，Web 内容被恶意修改，攻击者可以修改/替换文件等。

完整性影响的赋值如下：

（1）高：完整性完全丢失，或者完全丧失保护。例如，攻击者能够修改受影响组件中的任何文件。或者，攻击者只能修改一些文件，但是，恶意的修改能够给受影响组件带来直接的、严重的后果。

（2）低：攻击者可以修改数据，但是不能控制修改数据造成的后果，或者修改的数量是有限的。数据修改不会给受影响组件带来直接的、严重的影响。

（3）无：受影响组件的完整性没有丢失，攻击者不能修改受影响组件中的任何信息。

完整性影响为“高”表示攻击者能够修改/替换受影响组件中的任何文件，或者攻击者能够修改/替换他想修改的任何信息。或者，攻击者能够修改/替换一些关键信息，如管理员密码。

完整性影响为“低”表示攻击者只能修改/替换部分文件，不能任意修改/替换文件，也不能修改/替换关键文件。

3)可用性

这个指标度量漏洞的成功利用给受影响组件的性能带来的影响。机密性影响和完整性影响反映漏洞的成功利用对受影响组件数据的影响。例如，网络内容被恶意修改（完整性受影响），或系统文件被窃（机密性受影响）。可用性影响反映漏洞的成功利用对受影响组件操作的影响。

可用性影响的赋值如下：

（1）高：可用性完全丧失，攻击者能够完全拒绝对受影响组件中资源的访问。或者，攻击者可以拒绝部分可用性，但是能够给受影响组件带来直接的、严重的后果。例如，尽管攻击者不能中断已存在的连接，但是能够阻止新的链接；攻击者能够重复利用一个漏洞，虽然每个利用只能泄露少量的内

存，但是重复利用可以使一个服务变得不可用。

（2）低：攻击者能够降低资源的性能或者中断其可用性。即使能够重复利用这个漏洞，但是攻击者也不能完全拒绝合法用户的访问。受影响组件的资源是部分可用的，或在一些时候是完全可用的，但总体上不会给受影响组件带来直接的，严重的后果。

（3）无：受影响组件的可用性不受影响，攻击者不能降低受影响组件的性能。

例 6 在一个互联网服务如网页、电子邮件或 DNS 中的漏洞，该漏洞允许攻击者修改或删除目录中的所有文件。该漏洞的成功利用会导致完整性受影响，而可用性不会受到影响。这是因为网络服务仍然能正常执行，只是其内容被改变了。

可用性影响表示对服务自身性能和操作的影响，不是数据的影响。由于可用性是指信息资源的可访问性，因此消耗网络带宽、处理器周期或磁盘空间的攻击都会影响受影响组件的可用性。

可用性影响为“高”表示受影响的组件完全不能响应，完全不能正常工作、不能操作、不能提供服务。或者攻击者可以阻止新的访问，通过重复利用漏洞消耗受影响组件的资源使其不能进行正常的服务。

可用性影响为“低”表示受影响的组件的性能降低，部分服务受到影响，但不会造成完全不能工作。

3.2.2 时间度量

1)漏洞利用代码成熟度：可利用的代码或技术的状态。

2)修复级别

补救水平

3)报告可信度

目前所公布的缺陷以及已知技术细节的可信程度。

3.2.3 环境指标

CNNVD 漏洞影响实体描述规范

3.2.3.1 安全要求

一、定义

漏洞影响实体是描述安全漏洞信息时不可或缺的一个属性项，可以分为硬件、操作系统及应用程序等不同类型（部件）。根据漏洞影响实体组成类型不同及漏洞影响产品类型不同，用基本描述结构体和逻辑连接组合来对其进行描述。

二、描述原则

1) 通用性：能够描述所有的信息系统。

2) 一致性：相同组成部分的描述名称必须一致。

3) 概括性：能够概括具有某特点的一类信息系统。

4) 结构化：拥有清晰、分块、可读性高的描述格式。

5)　简易性：简化描述的名称和描述结构体。

三、适用范围

凡是被 CNNVD 漏洞库收录的漏洞，均适用此编码语法规范,包括采集的公开漏洞以及收录的未公开漏洞。

3.2.3.3 修改的基本指标

基本描述结构

基本描述结构是描述漏洞影响实体的命名方法，它由部件、生产厂商、产品名称、产品版本、更新版本、适用版本、界面语言等属性项组成，根据漏洞影响实体界面语言、主要应用国别等确定采用中文或英文进行描述，描述规则如下：

CNCPE:/{部件}:{生产厂商}:{产品名称}:{产品版本}:{更新版本}:{适用版本}:{界面语言}

CNCPE:/｛part｝:｛vendor｝:｛product｝:｛version｝:｛update｝:｛edition｝:｛language｝

该命名规则对于其中出现的英文名称大小写不敏感。各命名元素之间以英文冒号“:”作为分隔符，无空格。若对应项没有相关信息，允许空项，直接进入下一个分隔符；若对应项不适用于该产品，则该项填“-”。下面分别对各项进行说明。

1)部件

部件分为三类：硬件（Hardware）、操作系统（Operating system）和应用（Application）。

1、中文表达形式为：硬件、操作系统、应用。例如：

CNCPE:/应用:北京智通:网际快车:3.5:::中文-台湾

2、英文表达形式为：h、o、a。例如：

CNCPE:/a:acme:product:1.0:update2:-:en-us

2)生产厂商

生产厂商名称通常采用生产厂商的注册域名进行命名。

1、英文名称采用生产厂商所在最高组织的域名。

2、中文名称如果有中文域名，优先采用中文域名；如果只有英文域名，采用对应英文域名的中文翻译（如有）。

3、对于分享同一域名、不同后缀的生产厂商，采用域名的全称。

4、对于无特定域名的中国生产厂商，命名采用营业执照上的机构名称，省略公司性质字段。

5、对于无生产厂商的产品，生产厂商项采用开发者全名。英文单字间空格改为“_”，中文开发者采用其中文全名。

6、生产厂商名称随着厂家自身更名而更新。

生产厂商名称（附录 A.2）。

3)产品名称

产品名称依据生产厂商对产品的正式命名。

1、中英文产品名称通常保留全名，英文全名各个单词间用“_”相连。

2、对于具有官方惯用缩写且缩写不会引起名称混淆的产品名称，可以适当用英文缩写命名。

3、产品名称同产品全名的更新保持一致。

产品最通用或可识别的名称（附录 A.3）。

4)产品版本

使用厂商指定的版本号（附录 A.4），此处不应缩减或修改。但可以使用“*”“?”等通配符辅助描述版本号。

5)更新版本

更新版本反映同一产品版本下的更新情况或服务包信息，其表达往往因生产厂商和产品不同而不同，对此，一律按照生产厂家所规定的或产品自带的更新信息来表示。

使用厂商指定的更新号或名称（附录 A.5）。

6)适用版本

适用版本反映产品适用的对象或平台（附录 A.6）。其中，缩写规则参考（附录 A.8）。

7)界面语言

界面语言按照 IETF RFC 4646 Tags for Identifying Languages 中定义的语言标签来表示。（附录 A.7）。

逻辑连接符号

出于漏洞影响实体组成的复杂性，及漏洞影响的产品和版本多样性，上面的基本描述结构不能满足部分漏洞所影响的产品。

用“AND”（同时满足）、“OR”（满足任一）、“NOT”（不满足）三个逻辑连接符号连接不同的基本结构。

3.3 CVSS 等级结果

漏洞的危害可采用评分或分级的方式进行评价，漏洞的评分由可利用性指标组的评分和影响性指标组的评分两部分共同组成，漏洞的危害等级可根据其评分进行划分。

漏洞的分值在 0 到 10 之间，漏洞的评分规则如下：

（1）如果 可利用性评分 + 影响性评分 ＞10，漏洞评分 ＝10

（2）漏洞评分 ＝ 可利用性评分 + 影响性评分

（3）漏洞分值保留到小数点后 1 位，如果小数点后第二位的数字大于 0，则小数点后第一位数字加 1。

CNNVD 将漏洞的危害级别划分为四个等级，从高至低依次分为超危、高危、中危和低危，具体划分方式见表 4。

表 4 漏洞危害等级划分表

漏洞评分	漏洞等级
9.0-10	超危
7.0-8.9	高危
4.0-6.9	中危
0-3.9	低危

4.漏洞扫描报告

CNNVD-201304-152

漏洞名称：phpMyAdmin ‘tbl_gis_visualization.php’多个跨站脚本漏洞

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 3.5.0 至 3.5.7 版本中的 tbl_gis_visualization.php 中存在多个跨站脚本漏洞，该漏洞源于程序没有充分验证用户提供的输入。当用户浏览受影响的网站时，其浏览器将执行攻击者的任意脚本代码。这可能导致攻击者窃取基于 cookie 的身份认证并发起其它攻击。

影响范围	改变	脆弱性组件是phpMyAdmin，受影响组件是受害者的浏览器		
攻击途径	网络	脆弱性组件是web应用		
攻击复杂度	低	攻击者只需要对目标系统做一些简单的调查，一些需要的条件很容易获得		
权限要求	无	不需要权限就可以发动攻击		
用户交互	需要	需要受害者访问受影响的网站		
机密性影响	低	攻击者可以获取受害者web浏览器维护的信息，但局限于与运行phpMyAdmin的web站点有关联的信息		
完整性影响	低	攻击者可以修改受害者web浏览器维护的信息，但仅限于与运行phpMyAdmin的web站点有关联的信息		
可用性影响	无	恶意代码能够降低受害者浏览器的性能，但是影响通常很小并且受害者能够关闭浏览器中断影响		
漏洞评分		6.1	危害等级	中危

5.漏洞总数和剩余漏洞数

5.1 概述

一、描述定义

漏洞内容描述是指通过文字描述的方式把该漏洞产生的原因、存在的位置、受影响范围、漏洞宿

主介绍等按照统一的格式进行描述。

二、描述原则

1)简明易懂性：简明、清晰、易懂的对漏洞进行描述。

2)真实性：真实、客观的对该漏洞进行描述。

3)透明性：避免暴露过多的漏洞技术细节。

三、适用范围

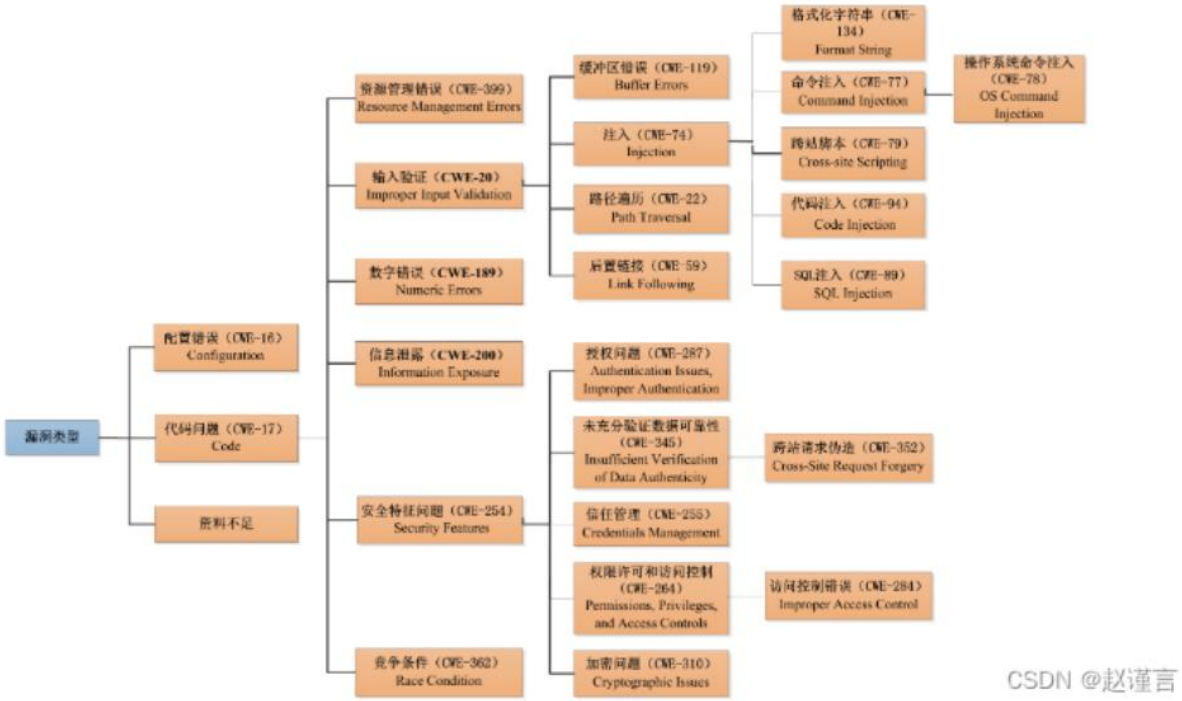
凡是被 CNNVD 漏洞库收录的漏洞，均适用此编码语法规范,包括采集的公开漏洞以及收录的未公开漏洞。

5.2 结果分析

5.3.1 漏洞扫描结果

5.3.1.1 任务概述

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。



图中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。

5.3.1.2 风险分布

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。

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）。

5.3.1.2 漏洞信息

漏洞内容描述办法

漏洞内容描述包括“受影响实体”和“漏洞内容”两个部分，规则如下：

受影响实体介绍 + 漏洞内容描述

1)受影响实体介绍

受影响实体介绍是指在描述漏洞信息之前，先要简述存在该漏洞的软件或产品的基本信息（如：该实体的所属、定义、功能等）；

格式规则

受影响实体名称+公司+受影响实体定义+功能概述

格式内容

XXX 实体是 XXX 国家 XXX（英文）公司的一款（量词） XXX 产品（软件、解决方案、系统、工具等）。该产品具有 XXX 的功能（适用范围、作用等）。

2)漏洞内容描述

漏洞内容描述是指简述该漏洞的类型、产生原因、漏洞的攻击方式及产生的影响等。

格式规则

漏洞类型+产生的原因+利用方式+影响版本

格式内容

漏洞类型：受影响实体存在某类型的漏洞；

产生的原因：造成漏洞的原因；

利用方式：攻击者以什么方式利用漏洞，及可能给系统、用户软件造成的影响；

影响版本：受影响实体的版本信息。

3)漏洞内容描述举例

以 Microsoft Exchange Server Outlook Web App 跨站脚本漏洞（CNNVD-201503-274）为例：

〖受影响实体名称〗Microsoft Exchange Server 是〖公司〗美国微软（Microsoft）公司的〖受影响实体定义〗一套电子邮件服务程序。

〖功能概述〗它提供邮件存取、储存、转发，语音邮件，邮件过滤筛选等功能。Outlook Web App（OWA）是其中的一个用于访问 Exchange 邮箱的 Web 浏览器版本。

〖漏洞类型〗Microsoft Exchange Server 中存在跨站脚本漏洞，〖漏洞产生的原因〗该漏洞源于程序无法正确整理 OWA 中的页面内容。

〖漏洞利用方式〗通过修改 OWA 中的属性，然后诱使用户浏览目标 OWA 站点，〖漏洞造成危害〗攻击者可在当前用户的上下文中运行脚本。以下产品及版本受到影响：Microsoft Exchange Server 2013 SP1，Cumulative Update 7。

以 Gnupg2 信息泄露漏洞（CNNVD-201503-085）为例：

〖受影响实体名称〗Gnupg2（GNU Privacy Guard）是〖公司〗GNU 计划开发的〖受影响实体定义〗一套开源的加密软件，采用 GNU 通用公共许可证。

〖功能概述〗该软件支持公钥、对称加密、散列等算法。

〖漏洞类型〗Gnupg2 中存在信息泄露漏洞。〖漏洞造成危害〗远程攻击者可利用该漏洞获取敏感信息的访问权限。

5.3.2 漏洞情况

报告名称：外部软件环境评估报告

报告机构：中国信息安全测评中心

提供方： 国家信息安全漏洞库

重要漏洞实例

漏洞类型	其他
漏洞编号	CNNVD-202211-3038
厂商	谷歌
漏洞实例	Google Android 安全漏洞
是否修复	是
危害等级	高危

漏洞简述

Google Android 安全漏洞（CNNVD-202211-3038）：

Google Android 是美国谷歌（Google）公司的一套以 Linux 为基础的开源操作系统。

Google Android 存在安全漏洞，该漏洞源于在 SharedMetadata.cpp 的 shared_metadata_init 函数中存在整数溢出问题，从而导致越界写入。攻击者利用该漏洞可以升级权限。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://source.android.com/docs/security/bulletin/pixel/2022-11-01

结论

已知漏洞总数	无
已知剩余漏洞总数	无
软件的影响	无
综合剩余风险	目前厂商已发布升级补丁以修复漏洞

根据文档的要求只能满足在 XXX 操作系统环境下运行。本软件自身不对外服务，操作系统禁用的本地服务。同时在国家公开漏洞库中已公开披露的漏洞，已知漏洞总数，已知剩余漏洞总数为 0，目前厂商已发布升级补丁修复漏洞，对本软件无任何影响。

6.剩余漏洞的维护方案

6.1 剩余漏洞情况

目前，官方已经发布了修复漏洞的升级版本，建议用户及时确认是否受到漏洞影响，尽快采取修补措施。

6.2 网络安全策略

操作系统安全建议 ：操作系统是运行应用程序的物理环境，操作系统中的任何漏洞可危害应用程序的安全性。通过保护操作系统安全，可以使环境稳定，控制资源的访问，以及控制环境的外部访问。

数据库安全建议：数据库软件漏洞属于产品自身的缺陷，由数据库厂商对其修复，通常以产品补丁的形式出现。

网络设备安全建议：

1、在产品发布前应对产品进行严格的安全测试；

2、及时关注最新的安全技术，及时修补产品中存在漏洞的第三方库等外部依赖。

总结

在漏洞态势不断发生变化的大环境中，新华三秉承维护计算机网络空间安全的核心理念，从漏洞的视角针对目前的安全建设提出一些建议。对于安全建设有一些公共安全建议，例如及时安装系统和软件的更新补丁，隔离办公网和生产环境，主机进行集成化管理，配置防护系统实时在网络传输层进行链路阻断，禁止外部 IP 访问特殊端口（如 139、445、3389 端口），采用最小化端口与服务暴露原则等。对于各个不同分类漏洞，安全建议不尽相同。