CNNVD漏洞分级规范

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。

三、漏洞评分指标

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。

（一）可利用性指标组

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. 攻击途径

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. 攻击复杂度

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. 权限要求

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。

表 1 不同操作系统中权限要求评分参考表

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”。

（二）影响性指标组

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. 机密性影响

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. 完整性影响

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. 可用性影响

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。

四、评分与评级

（一）可利用性指标组的评分

可利用性指标组中各个指标的不同取值的组合有不同的评分，表 2给出了具体的评分情况。

表 2 可利用性指标组的评分表

攻击途径	攻击复杂度	权限要求	用户交互	可利用性指标评分	
				范围不变	范围改变
网络	低	无	不需要	3.89	4.20
网络	低	无	需要	2.84	3.06
网络	低	低	不需要	2.84	3.36
网络	低	低	需要	2.07	2.45
网络	低	高	不需要	1.23	2.47
网络	低	高	需要	0.90	1.80
网络	高	无	不需要	2.22	2.40
网络	高	无	需要	1.62	1.75
网络	高	低	不需要	1.62	1.92
网络	高	低	需要	1.18	1.40
网络	高	高	不需要	0.71	1.41
网络	高	高	需要	0.51	1.03
邻接	低	无	不需要	2.84	3.06
邻接	低	无	需要	2.07	2.23
邻接	低	低	不需要	2.07	2.45
邻接	低	低	需要	1.51	1.79
邻接	低	高	不需要	0.90	1.80

邻接	低	高	需要	0.66	1.31
邻接	高	无	不需要	1.62	1.75
邻接	高	无	需要	1.18	1.28
邻接	高	低	不需要	1.18	1.40
邻接	高	低	需要	0.86	1.02
邻接	高	高	不需要	0.51	1.03
邻接	高	高	需要	0.38	0.75
本地	低	无	不需要	2.52	2.72
本地	低	无	需要	1.83	1.98
本地	低	低	不需要	1.83	2.17
本地	低	低	需要	1.34	1.59
本地	低	高	不需要	0.80	1.60
本地	低	高	需要	0.58	1.17
本地	高	无	不需要	1.44	1.55
本地	高	无	需要	1.05	1.13
本地	高	低	不需要	1.05	1.24
本地	高	低	需要	0.76	0.91
本地	高	高	不需要	0.46	0.91
本地	高	高	需要	0.33	0.67
物理	低	无	不需要	0.91	0.99
物理	低	无	需要	0.67	0.72
物理	低	低	不需要	0.67	0.79
物理	低	低	需要	0.49	0.58
物理	低	高	不需要	0.29	0.58
物理	低	高	需要	0.21	0.42
物理	高	无	不需要	0.52	0.56
物理	高	无	需要	0.38	0.41
物理	高	低	不需要	0.38	0.45
物理	高	低	需要	0.28	0.33
物理	高	高	不需要	0.17	0.33
物理	高	高	需要	0.12	0.24

（二）影响性指标组的评分

影响性指标组中各个指标的不同取值的组合有不同的评分，表 3给出了具体的评分情况。

表 3 影响性指标组的评分表

机密性影响	完整性影响	可用性影响	影响性指标评分	
			范围不变	范围改变
高	高	高	5.87	6.53
高	高	低	5.45	6.45
高	高	无	5.18	6.22
高	低	高	5.45	6.45
高	低	低	4.70	5.69
高	低	无	4.22	5.09
高	无	高	5.18	6.22
高	无	低	4.22	5.09
高	无	无	3.60	4.31
低	高	高	5.45	6.45
低	高	低	4.70	5.69
低	高	无	4.22	5.09
低	低	高	4.70	5.69
低	低	低	3.37	4.03
低	低	无	2.51	2.94
低	无	高	4.22	5.09
低	无	低	2.51	2.94
低	无	无	1.41	1.55
无	高	高	5.18	6.22

无	高	低	4.22	5.09
无	高	无	3.60	4.31
无	低	高	4.22	5.09
无	低	低	2.51	2.94
无	低	无	1.41	1.55
无	无	高	3.60	4.31
无	无	低	1.41	1.55
无	无	无	0.00	0.00
注：最后一种组合对机密性、完整性和可用性均无影响，忽略此组合。				

（三）漏洞评分与分级

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。

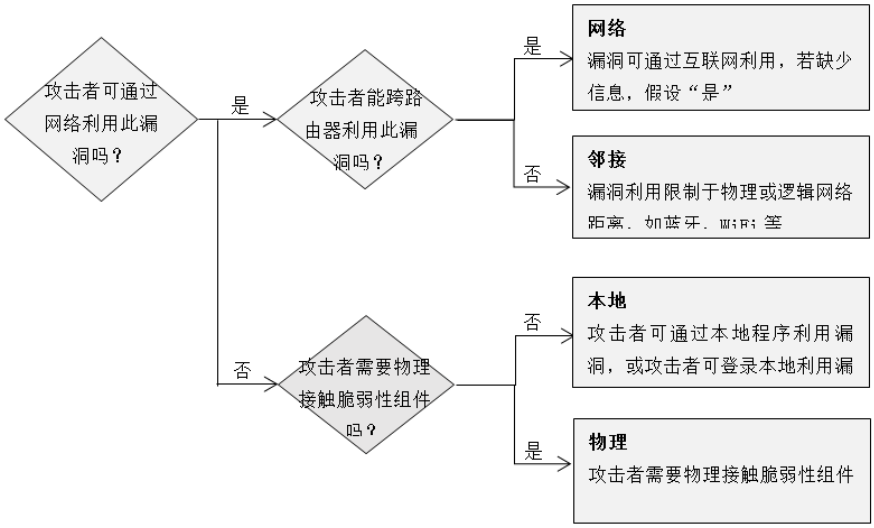
表 4 漏洞危害等级划分表

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

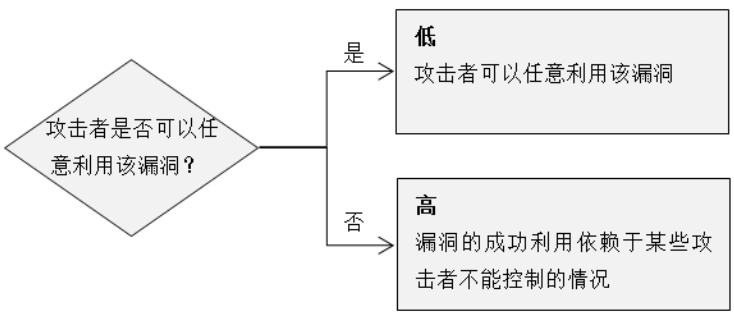
附录一：漏洞评分指标取值的判断方法

（一）可利用性指标组

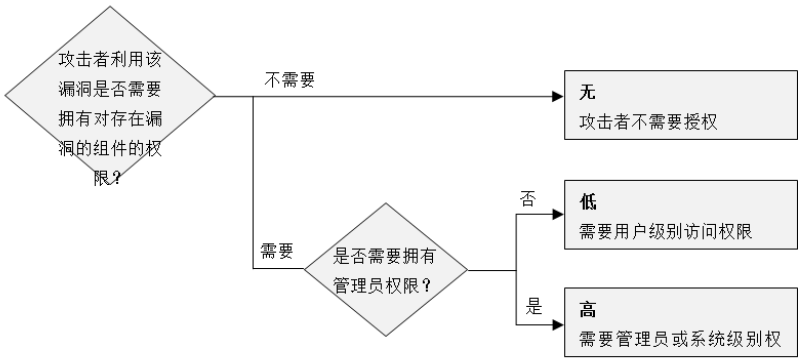
1. 攻击途径



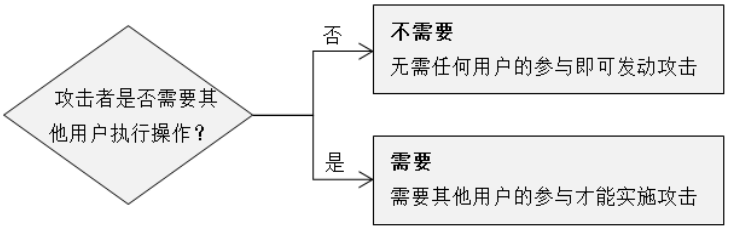
2. 攻击复杂度



3. 权限要求

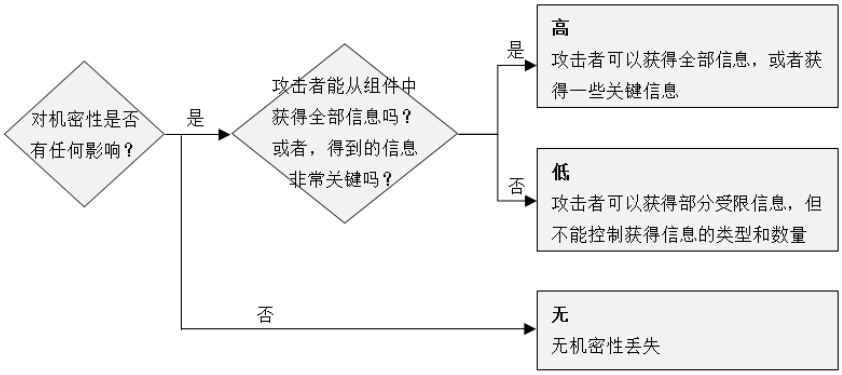


4. 用户交互

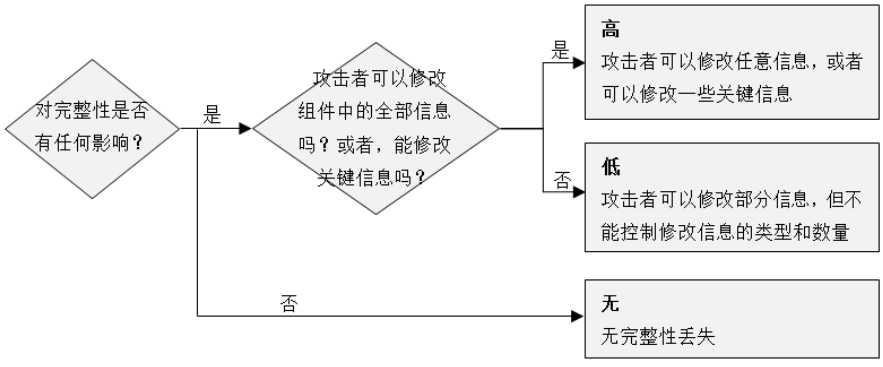


（二）影响性指标组

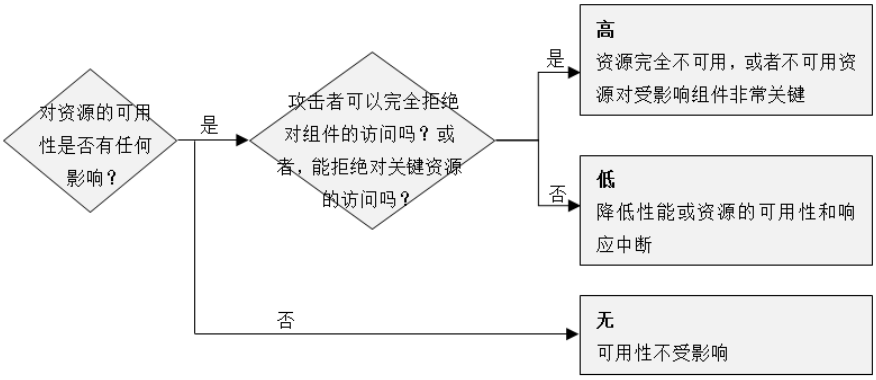
1. 机密性影响



2. 完整性影响



3. 可用性影响



附录二：漏洞危害评价实例

1. 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

2. CNNVD-201205-093

漏洞名称：VMware ESXi/ESX ‘VMX’ 进程拒绝服务漏洞

漏洞简介：

VMware ESXi 是简单快捷免费的实施虚拟化的方案，VMware ESX是美国威睿（VMware）公司的虚拟服务器系统。

VMware ESXi 3.5至4.1版本与ESX 3.5至4.1版本中的VMX进程中存在漏洞，该漏洞源于未正确处理RPC命令。guest操作系统用户可利用该漏洞借助涉及数据指针的向量导致拒绝服务（内存重写与进程崩溃），或者在主机操作系统上执行任意代码。

影响范围	改变	脆弱性组件是一个VMX进程，受影响组件是主机操作系统	
攻击途径	网络	VMX进程在网络栈，攻击者可远程发送RPC命令	
攻击复杂度	低	要求虚拟机有4GB内存，低于4GB内存的虚拟机不受影响	
权限要求	低	攻击者需要guest权限	
用户交互	不需要	攻击者可在任意时刻发送RPC命令，不需要用户参与	
机密性影响	高	攻击者可在主机操作系统上执行任意代码	
完整性影响	高	攻击者可在主机操作系统上执行任意代码	
可用性影响	高	攻击者可在主机操作系统上执行任意代码，导致拒绝服务	
漏洞评分		9.9	危害等级	超危

3. CNNVD-201310-631

漏洞名称：Juniper Junos 信息泄露漏洞

漏洞简介：

Juniper Networks Juniper Junos是美国瞻博网络（Juniper Networks）公司的一套专用于该公司的硬件系统的网络操作系统。该操作系统提供了安全编程接口和Junos SDK。

Juniper Junos中存在信息泄露漏洞，在unnumbered接口上启用Proxy ARP时，远程攻击者可通过特制的ARP消息利用该漏洞实施ARP投毒攻击，也可能获取敏感信息。以下版本受到影响：Juniper Junos 10.4，11.4，11.4X27，12.1，12.1X44，12.1X45，12.2，12.3，13.1。

影响范围	改变	脆弱性组件是Junos设备自身，受影响组件是感染ARP的所有设备
攻击途径	邻接	漏洞利用局限于局域网
攻击复杂度	低	攻击者构造ARP包的复杂度低
权限要求	无	无权限要求

用户交互	无	不需要用户交互	
机密性影响	高	攻击者可读取目标用户的任意网络数据	
完整性影响	无	攻击者不能修改目标用户的网络数据	
可用性影响	高	可造成受影响组件完全拒绝服务	
漏洞评分	9.3	危害等级	超危

4. CNNVD-200902-480

漏洞名称：Adobe Acrobat和Reader PDF文件处理缓冲区溢出漏洞

漏洞简介：

Adobe Acrobat和Reader都是非常流行的PDF文件阅读和编辑器。

如果用户受骗使用Adobe Acrobat和Reader打开了畸形的PDF文档，就可以触发缓冲区溢出，导致执行任意代码。Acrobat集成于流行的Web浏览器，访问网站就足以导致Acrobat加载PDF内容。目前这个漏洞正在被木马积极的利用。

影响范围	改变	脆弱性组件是Adobe Acrobat和Reader，受影响组件是本地系统	
攻击途径	本地	本地软件包含漏洞，需要通过打开畸形文档才能触发漏洞	
攻击复杂度	低	不需要特定的条件	
权限要求	无	无权限要求	
用户交互	需要	需要用户打开畸形文档	
机密性影响	高	考虑最坏情况，若受害者有管理员权限，对系统的机密性影响高	
完整性影响	高	考虑最坏情况，若受害者有管理员权限，对系统的完整性影响高	
可用性影响	高	考虑最坏情况，若受害者有管理员权限，对系统的可用性影响高	
漏洞评分	8.6	危害等级	高危

5. CNNVD-201402-235

漏洞名称：Apple iOS iCloud 权限许可和访问控制漏洞

漏洞简介：

iCloud是美国苹果（Apple）公司的一款云服务，它支持存储音乐、照片、App和联系人等。

Apple iOS 7.04及之前的版本中的iCloud子系统中存在安全漏洞。物理位置临近的攻击者可通过输入任意iCloud Account Password和空的iCloud Account Description值利用该漏洞绕过既定的密码要求。关闭Find My iPhone服务或完成Delete Account操作，并使用其他的Apple ID账户关联此服务。

影响范围	不改变	脆弱性组件和受影响组件均是iCloud子系统	
攻击途径	物理	攻击者需要物理接触设备	
攻击复杂度	低	攻击步骤简单	
权限要求	无	考虑最坏情况，假设设备没有使用PIN保护	
用户交互	不需要	不需要用户交互	
机密性影响	无	该漏洞不会造成直接的机密性影响	
完整性影响	高	由于该功能的重要性，因为完整性影响高	
可用性影响	无	该漏洞不会造成直接的可用性影响	
漏洞评分	4.6	危害等级	中危

6. CNNVD-201406-080

漏洞名称：OpenSSL 加密问题漏洞

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中存在安全漏洞，该漏洞源于程序没有正确限制ChangeCipherSpec消息的处理。攻击者可借助特制的TLS握手利用该漏洞实施中间人攻击，在OpenSSL-to-OpenSSL通信过程中使用零长度的主密钥，劫持会话或获取敏感消息。以下版本受到影响：OpenSSL 0.9.8y及之前的版本，1.0.0m之前的1.0.0版本，1.0.1h之前的1.0.1版本。

影响范围	不改变	脆弱性组件和受影响组件均是OpenSSL	
攻击途径	网络	OpenSSL是网络应用，攻击者可远程利用该漏洞	
攻击复杂度	高	攻击者必须能够监视和修改受害者的网络数据	
权限要求	无	无权限要求	
用户交互	不需要	不需要用户交互	
机密性影响	高	攻击者能够解密客户端和服务器间所有的SSL/TLS通信数据	
完整性影响	高	攻击者能够解密客户端和服务器间所有的SSL/TLS通信数据	
可用性影响	无	不会对SSL/TLS回话造成可用性影响	
漏洞评分	7.4	危害等级	高危

数据文件