CNNVD漏洞内容描述规范

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。

四、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。