西门子S7-200晶体管模块CPU226CN

产品名称	西门子S7-200晶体管模块CPU226CN
公司名称	浔之漫智控技术（上海）有限公司
价格	.00/件
规格参数	品牌:西门子 型号:全系列 产地:德国
公司地址	上海市松江区石湖荡镇塔汇路755弄29号1幢一层A区213室
联系电话	15721261077 15721261077

产品详情

西门子S7-200晶体管模块CPU226CN

访问路径的赋值包括本地、邻接和远程，通常可被远程利用的安全漏洞危害程度高于可被邻接利用的安全漏洞，可本地利用的安全漏洞次之。利用复杂度的赋值包括简单和复杂，通常利用复杂度为简单的安全漏洞危害程度高。影响程度的赋值包括完全、部分、轻微和无，通常影响程度为完全的安全漏洞危害程度高于影响程度为部分的安全漏洞，影响程度为轻微的安全漏洞次之，影响程度为无的安全漏洞可被忽略。影响程度的赋值由安全漏洞对目标的机密性、完整性和可用性三个方面的影响共同计算。攻击者指定的任意指令或命令，控制应用系统或操作系统。这种漏洞威胁西门子大，同时影响系统的机密性、完整性，甚至在需要的时候可以影响可用性。主要来源为内存破坏类。

2）获取信息。即可以导致劫持程序访问预期外的资源并泄露给攻击者，影响系统的机密性。主要来源为输入验证类和配置错误类漏洞。

3）拒绝服务。即可以导致目标应用或系统暂时或永远性地失去响应正常服务的能力，影响系统的可用性。主要来源为内存破坏类和意外处理错误类漏洞。

2.2.2 软件漏洞的分级

对漏洞进行分级，有助于人们对数目众多的安全漏洞给予不同程度的关注并采取不同级别的措施，因此，建立一个灵活、协调一

致的漏洞级别评价机制是非常必要的。

如今，各漏洞发布组织和技术公司都有自己的评级标准。目前主要的漏洞级别评价方式有按照漏洞严重等级和利用漏洞评分系统（CVSS）进行分级两类主要形式。引用的错误解析、异常处理失败、违反代码

编写标准，以及消息或数据结构的不当处理等。额，国内大量软件开发厂商对软件开发过程的管理不够重视，大量软件使用开源代码和公用模块，缺陷率普遍偏高对软件安全漏洞进行分类是搜集威胁信息、掌握安全威胁发展趋势的基础。更全面、精细的软件安全漏洞分类可以把安全事件、漏洞利用和软件平台等多方面组件在安全的视角下关联起来，从而帮助安全专家、分析人员等有效地进行分析，找到相应的解决方案。漏洞的分类是客观存在的，但不是一成不变的，而是根据需求变化的。，可被利用的已知和未知缺陷较多。

软件公司中，项目管理和软件开发人员缺乏软件安全开发知识，不知道如何更好地开发安全的软件。实施软件的安全开发过程，需要开发团队所有的成员及项目管理者都具备较高的安全知识。软件开发人员很少进行安全能力与意识的培训，项目开发管理者不了解软件安全开发的管理流程和方法，不清楚安全开发过程中使用的各类方法和思想；开发人员大多数仅学会了编程技巧，不了解安全漏洞的成因、技

软件开发生命周期的各个环节都是人为参与的，经验的缺乏和意识的疏忽都有可能引入安全漏洞。为此，本书用以培养软件开发人员的安全开发意识，增强对软件安全威胁的认识，提高安全开发水平，提升IT产品和软件系统的抗攻击能力经常仓促发布软件。软件开发人员将软件功能视为头等大事，对软件安全架构、安全防护措施认识不够，只关注是否实现需要的功能，很少从“ 攻击者 ”的角度来思考软件安全问题。

如果采用严格的软件开发质量管理机制和多重测试技术，软件公司开发的产品的缺陷率会低很多。在软件安全性分析中可以使用缺陷密度（即每千行代码中存在的软件缺陷数量）来衡量软件的安全性。以下各类软件代码缺陷的统计数据也说明了这个情况。通常由程序员人工完成，导致漏洞的引入成为必然。当今软件和网络系统的高度复杂性，也决定了不可能通过技术手段发现所有的漏洞。

伴随信息技术的发展出现了很多新技术和新应用，如移动互联网、物联网、云计算、大数据和社交网络等。随着移动互联网、物联网的出现，网

端的数量呈几何倍数增长，云计算和大数据的发展极大提高了攻击者的计算能力，社交网络为攻击者提供了新的信息获取途径。总之，这些新技术、新应用不仅扩展了互联网影响范围，提高了互联网的复杂度，也增大了漏洞产生的概率，必然会导致越来越多的漏洞的产生。安全协议实现，以及云计算、移动智能终端中出现的新型软件漏洞分析，请扫描封底的二维码获取内容查看。4.软件使用场景更具威胁

网络技术拓展了软件的功能范围，提高了其使用方便程度，与此同时，也给软件带来了更大风险。由于软件被应用于各种环境，面对不同层次的使用者，软件开发者需要考虑更多的安全问题。同时，黑客和恶意攻击者可以比以往获得更多的时间和机会来访问软件系统，并尝试发现软件中存在的安全漏洞。

当前黑客组织非常活跃，其中既包括传统的青少年黑客、跨国黑客组织，也包括商业间谍黑客和恐怖主义黑客，乃至国家网络战部队。以前的黑客多以恶作剧和破坏系统为主，包括对技术好奇的青少年黑客和一些跨国黑客组织；现今的黑客则多为实施商业犯罪并从事地下黑产，危害已经不限于让服务与系统不可用，更多的是带来敏感信息的泄露和现实资产的损失。尤其是近些年，一系列APT攻击的出现及美国“ 棱