附件 5

《通用处理器芯片硬件漏洞分类分级标准》
标准编制说明

通用处理器芯片硬件漏洞分类分级标准标准起草组

XXXX 年 XX 月 XX 日

1、　　标准范围。

本文件给出了通用处理器芯片硬件漏洞（简称“漏洞”）的分类方式、分级指标及分级方法指南。其中，通用处理器指的是采用冯诺依曼结构的处理器，体系结构如图 1 所示。芯片包括独立的通用处理器芯片和片上系统中的通用处理器部分。硬件漏洞是指由处理器逻辑设计引入的，会对处理器功能正确性或安全性造成影响的设计缺陷。

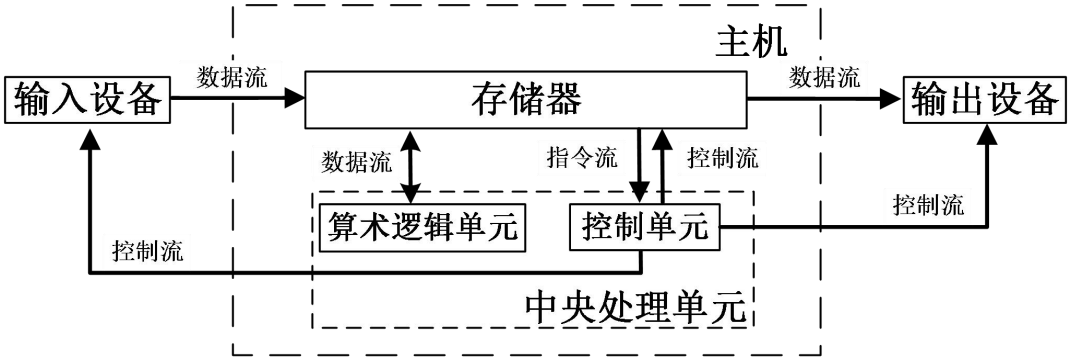

图 1 冯诺依曼体系结构

本标准适用于通用处理器芯片产品提供者、设计工具提供者、产品使用者、漏洞收录组织、漏洞应急组织在漏洞信息管理、芯片产品生产、技术研发、系统运营等相关活动中进行的漏洞分类、漏洞危害等级评估等工作。

2、　　工作简况。

处理器芯片的硬件安全是软件和系统安全的根基。自“熔断”、“幽灵”、“骑士”等漏洞曝光以来，涉及处理器权限正确性、数据完整性、信息私密性的安全问题日益严峻，全球数以亿计的计算设备的安全根基面临重大危机。

在我国，随着数字经济、新基建等国家战略的提出，关键信息基础设施中采用了大量的进口和国产处理器芯片，存在严重的“安全现

状不清、安全前景不明”的隐患，亟需针对这些处理器芯片的硬件漏洞开展研究。

2020 年以来，国家计算机网络应急技术处理协调中心（以下简称 CNCERT）先后参与和牵头了工信部创新发展工程“嵌入式芯片安全检测平台”和科技部重点研发计划“纳米级芯片硬件安全综合评估关键技术研究”两个项目，对芯片中的硬件安全问题开展深入研究。依托 CNCERT 建设的 CNVD 漏洞共享平台，编制组针对处理器硬件漏洞开展收录和分析工作。此外，由于处理器芯片硬件漏洞与其硬件实现方式有关，修复困难且修复方法对性能影响较大，因此项目组研究了针对处理器芯片硬件漏洞风险的评分标准，指导芯片厂商和应用单位进行针对性的修复。

现有的漏洞评分体系，大多面向软件和网络层面的漏洞，在应用到处理器上时，有两方面问题，一是对处理器芯片硬件漏洞的区分度不高，处理器厂商及应用单位难以参考；二是部分分类方式和技术评价指标不适用于处理器芯片。因此，本标准旨在设计一种适用于处理器芯片硬件漏洞的评分标准，可有效评价不同漏洞的攻击复杂度及危害性，从而对处理器芯片硬件漏洞的风险有更准确的评价。

3、标准编制原则和确定标准主要内容的依据：

该标准编制时的主要原则首先是主要的评分思想与软件的漏洞评分原则保持一致。本标准主要参考了软件漏洞评分的原则，从漏洞利用难度和漏洞影响程度两方面对漏洞进行评分。漏洞利用难度越大、漏洞影响程度越重，漏洞评分越高。在漏洞利用难度和漏洞影响程度

的细分指标上，本标准根据硬件漏洞的特点进行了进一步设计。

其次，考虑到芯片硬件漏洞的严重程度与其应用场景有较大关系，且芯片漏洞的修复将对性能产生潜在影响。因此，本标准增加了修复必要性评价指标，将应用场景的特点和需求纳入评价指标体系，供应用方根据实际需求，判断对硬件漏洞修复的必要性。

4、主要试验（或验证）的分析、综述报告。

本标准编制过程中，对主要的处理器硬件漏洞进行了分析评价，相关评价示例在附录中给出，评价结果与处理器芯片厂商给出的结果一致。

5、标准在起草过程中遇到的问题及解决办法：重大分歧意见的处理经过和依据：有无重要技术问题需要说明。

无。

6、与国外标准的关系：包括：采用国际标准和国外先进标准的程度，与国外标准主要技术内容的差异（可引用标准前言的内容）：

该标准项目参考了国际上对软件和网络漏洞评价的标准通用漏洞评分体系（Common Vulnerability Scoring System，CVSS）。该标准从被利用性和影响程度两个方面评价漏洞基础分，同时也将应用环境因素纳入修复必要性的评分指标，可随应用场景的变化评估是否有必要修复该漏洞。然而该评分标准中的一些评分要素不适用于处理器芯片硬件漏洞。因此，本标准在参考其整体评分框架的基础上，针对性的设计了面向处理器芯片硬件的评分要素。

7、修订标准时，说明与标准前一版本的重大技术变化，并列出所涉及的新、旧版本的有关章条（可引用标准前言的内容）：废止/代

替现行有关标准的建议：

不涉及。

8、说明标准与其他标准或文件的关系（可引用标准前言的内容），特别是与有关的现行法律、法规和强制性国家标准的关系：

目前国内尚没有面向处理器芯片硬件漏洞的评价标准。与该标准相关性较强的国家标准为《GB/T 30279-2020 信息安全技术 网络安全漏洞分类分级指南》，主要规定了软件和网络漏洞的分类、分级、评分方法。该标准项目对上述标准是一个补充，在评分框架上尽量与其保持一致，但在评分要素上，针对处理器芯片硬件漏洞的特点进行了调整。

9、标准作为强制性标准或推荐性标准的建议：

建议作为推荐性标准。

10、贯彻国家标准的要求和措施建议（包括组织措施、技术措施、过渡办法等内容）：标准发布后，对国内外业界可能产生的影响。

标准发布后，CNCERT 芯片硬件漏洞库将依据该标准，对处理器芯片硬件漏洞进行分级分类管理。漏洞发现者、处理器芯片厂商、处理器芯片应用方均可参考该标准，对发现的芯片硬件漏洞进行处置。

11、标准是否涉及知识产权的情况说明；如标准中含有自主知识产权，说明产品研发程度、产业化基础及进程。

无。

12、其他应予说明的事项。

无。