ICS 35.160
CCS L62

团 体 标 准

T/ISC 0061—2024

通用处理器芯片硬件漏洞分类分级标准

Standard for Common Central Processing Unit Integrated Circuit Hardware Vulnerability Classification and Rating

2024－09－03 发布 2024－10－03 实施

中 国 互 联 网 协 会 发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中国互联网协会提出并归口。

本文件起草单位：国家计算机网络应急技术处理协调中心、清华大学、西北工业大学、中国科学院微电子研究所、北京邮电大学、天津大学、龙芯中科技术股份有限公司、南京集成电路设计服务产业创新中心有限公司、广州大学。

本文件主要起草人：张家琦、何跃鹰、汪东升、吕勇强、胡伟、邓辰辰、赵发展、孙中豪、李莹、邱朋飞、何家骥、汪文祥、罗召建、鲁辉、李默涵。

本文件及其所代替文件的历次版本发布情况为：

——

引　言

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“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。在我国，关键信息基础设施中存在大量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。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，因此亟需研究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。

在进行漏洞分级指标量化赋分时，本标准从两方面对量化方法进行设计。一是参考现有漏洞评价体系，从被利用性和影响程度两方面进行计算，相关公式参考了文献[1][2]及标准《网络安全漏洞分类分级指南》（GB/T 30279）的计算方法。二是在一些新指标的赋分量化上，由于目前芯片硬件漏洞数量较少，因此主要采纳领域内专家意见，对指标量化赋分进行定义。

此外，由于本标准主要目标是对硬件漏洞的危害进行评分，漏洞对不同平台和架构的影响程度，将在漏洞库收录时，在影响产品条目中予以体现，因此在考虑漏洞危害时，未将在不同平台架构中的可移植性或者可复现性纳入考虑。

通用处理器芯片硬件漏洞分类分级标准

1 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。

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 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 20984 信息安全技术 信息安全风险评估规范

GB/T 22186 信息安全技术 具有中央处理器的IC卡芯片安全技术要求

GB/T 25069 信息安全技术 术语

GB/T 28458 信息安全技术 安全漏洞标识与描述规范

GB/T 30276 信息安全技术 安全漏洞管理规范

GB/T 30279 信息安全技术 网络安全漏洞分类分级指南

GB/T 40653 信息安全技术 安全处理器技术要求

GB/T 39786 信息安全技术 信息系统密码应用基本要求

GB/T 37092 信息安全技术 密码模块安全要求

GB/T 37720 信息技术 识别卡—金融IC卡芯片技术要求

中国金融集成电路（IC）卡规范（V3.0）

3 术语和定义

GB/T25069、GB/T 20984、GB/T 30276和GB/T 30279中界定的以及下列术语和定义适用于本文件。

3.1

通用处理器 General Central Processing Unit

采用冯诺依曼体系结构的现代处理器，包括运算器、控制器、存储器等基本处理器结构

3.2

硬件漏洞 Hardware Vulnerability

由硬件设计和实现方式缺陷引入的漏洞，硬件设计方式主要包括电路设计和微架构设计，硬件实现指设计经电子设计自动化流程转化为物理电路的过程。

3.3

知识产权核 Intellectual Property Core

芯片设计中可以重复使用，具有知识产权的集成电路设计功能模块

3.4

微架构 Microarchitecture

指令集架构的具体实现，它包括了中央处理器的内部结构、执行单元、缓存、流水线等。

4 符号和缩略语

下列符号和缩略语适用于本文件。

CPU 中央处理器（Central Processing Unit）
IP 知识产权（Intellectual Property）
I/O 输入/输出（Input/Output）
VM 虚拟机（Virtual Machine）
SMM 系统管理模式（System Management Mode）

5 通用处理器芯片硬件漏洞分类

5.1 概述

通用处理器芯片硬件漏洞主要包含处理器芯片设计和实现阶段引入的硬件安全脆弱性，通常存在于集成电路设计、微架构设计和芯片I/O接口上，这类脆弱性通常难以直接通过软件进行修复。

通用处理器芯片硬件漏洞分类是基于漏洞产生或触发的技术原因进行的划分。本文件采用树形导图对漏洞进行分类，首先从根节点开始，根据漏洞成因将漏洞归入某个具体的类别，如果该类型节点有子类型节点，且漏洞成因可以归入该子类型，则将该漏洞划分为该子类型，如此递归，直到漏洞归入的类型无子类型节点或漏洞不能归入子类型为止。

5.2 电路设计缺陷

5.2.1 概述

此类漏洞指处理器芯片设计代码开发过程中，因电路层设计或实现不当而导致的漏洞。

5.2.2 知识产权核不可信

处理器芯片中集成的知识产权核存在安全缺陷，或错误连接和使用知识产权核，导致该知识产权核可以访问其他电路中的私密信息，或恶意修改电路中存储的信息。

5.2.3 锁死保护逻辑功能错误

寄存器等锁死位保护功能设计漏洞，攻击者可以在用户设定锁死位寄存器之后，修改该寄存器设置。

5.2.4 控制逻辑控制错误

电路实现中的控制逻辑如有限状态机、比较逻辑、仲裁逻辑等存在缺陷，使其存在与预期行为不符的控制逻辑。

5.2.5 竞争冒险条件

电路设计中，存在竞争冒险情况，导致电路层面出现信号状态不符合设计规范。

5.2.6 信号缺乏保护机制

电路设计中，缺乏对多级电压、可调节时钟和电源及时钟毛刺的检查。

5.2.7 恶意逻辑及设计后门

存在恶意逻辑设计或未公开的设计功能，激活情况下，可导致电路执行非预期的操作。

5.2.8 其他电路设计缺陷

不能被归为上述类别的其他电路设计缺陷。

5.3 微架构设计缺陷

5.3.1 预测执行机制缺陷

现代处理器通常采用乱序执行、预测、预先取值、数据转发、缓存等技术来提高性能。这些技术的硬件实现方式，导致在执行中间状态时，存在安全上的隐患。一些高性能部件，包括缓存、分支预测逻辑、存储或加载缓存，存在泄露信息的可能性。预测执行和乱序执行为攻击者提供了对数据通过侧信道泄露的攻击渠道。

5.3.2 资源共享机制缺陷

在共享资源上，由于错误的访问控制逻辑、信息未及时清理等问题，导致攻击者可以访问非授权信息。

5.3.3 侧信道和隐蔽信道

处理器存在侧信道或隐蔽信道，使得处理器芯片内部的状态或数据信息与时间、功耗等信息具备一定的相关性，导致攻击者可非法获取芯片内部信息。

5.3.4 安全流程设计缺陷

处理器安全流程设计瑕疵导致的缺陷，例如没有启动访问控制前，过早启用DMA、启动过程缺乏认证等。

5.3.5 指令序列的非预期行为

处理器的某些指令序列导致处理器执行后出现了非预期行为。

5.3.6 不正确的故障处理逻辑

出现电压、时钟、指令等故障时，未能正确处理故障，导致攻击者可以进行非法操作。

5.3.7 其他微架构设计缺陷

不能被归为上述类别的其他微架构设计缺陷。

5.4 配置缺陷

5.4.1 未定义的配置功能

处理器的配置、控制、状态寄存器以及处理器的某些行为，出现了处理器功能描述中未定义的功能。

5.4.2 非预期的寄存器配置行为

寄存器的配置行为与其预期行为不符，如电源状态转换后的不正确锁定行为。

5.4.3 不安全的状态切换

处理器未正确地清除配置状态，从而导致不正确的执行行为。

5.4.4 不安全的权限管理和访问控制

硬件设计中存在缺陷导致用户的权限管理和访问控制策略与预期不符。

5.4.5 其他配置缺陷

不能被归为上述类别的其他处理器配置缺陷。

5.5 密码应用缺陷

5.5.1 不安全的密码算法

密码算法安全性低，包括使用已废止的密码算法标准，现行算法标准强度未达到应用安全等级，密钥等密码算法参数达到应用安全要求，或密码算法存在弱密钥、密钥互补对称性、差分攻击、代数攻击、迭代攻击等设计脆弱性。

5.5.2 未实现密码算法中所需的所有步骤

加解密模块未实现密码算法中所需的所有步骤（如轮数不够），导致生成了弱于算法公布的加密能力的结果，或选用了低安全级别的加密工作模式，或使用了未受保护的存储单元保存密钥或密码运算中间结果。

5.5.3 密码实现成为解密载体

密码模块能够实现数据的安全加密和安全加密存储，但对解密数据未作有效管控，导致解密后的明文泄露，密码模块成为被攻击者利用的解密载体。

5.5.4 可预测的随机数发生机制

伪随机数生成算法输出随机性不达标，或通过有限的随机序列可准确预测随机数发生器输出，或未按照要求设置随机数种子，或随机数源受干扰后随机性显著下降。

5.5.5 不安全的密钥管理

加解密模块的密钥存储在不安全的位置，或未按照时限要求更换密钥，或攻击者可以替换工作密钥。

5.5.6 未采用侧信道防护机制

密码模块缺乏物理或逻辑侧信道防护机制，导致加密运算侧效应可观测和敏感信息泄露。

5.5.7 其他加解密实现缺陷

不能被归为上述类别的其他加解密实现缺陷。

6 通用处理器芯片硬件漏洞分级

6.1 概述

通用处理器芯片硬件漏洞分级根据场景不同，分为危害分级和修复必要性分级两种分级方式。

危害分级均包括超危、高危、中危和低危四个等级，反映特定产品的漏洞危害程度，从漏洞本身的技术特点对其危害程度进行等级划分，主要面向漏洞分析人员、产品开发人员。

修复必要性分级反映在特定时期特定环境下的漏洞修复的必要性，用于在特定系统、特定场景下，考虑特定应用需求情况下，对漏洞修复的必要性进行划分，主要面向处理器应用方。

漏洞危害分级和修复必要性分级均可对单一漏洞进行分级，也可对多个漏洞构成的组合漏洞进行分级。

通用处理器芯片硬件漏洞分级包括分级指标和分级方法两方面内容。分级指标主要阐述反映漏洞特征的属性和赋值，包括被利用性指标、影响范围指标和环境因素指标三类。分级方法主要阐述技术分级和综合分级的具体步骤和方法，包括漏洞指标类评级方法、漏洞技术分级方法和漏洞综合分级方法。其中漏洞指标类评级方法是对上述三类指标进行评级的方法，是漏洞技术分级和综合分级的重要步骤。

6.2 漏洞分级指标

6.2.1 被利用性

6.2.1.1 攻击途径

攻击途径指利用漏洞的途径。攻击途径的赋值包括软件利用和硬件利用。通常，软件利用的可利用性高于硬件利用。见表 1。

表 1 攻击途径赋值说明表

赋值	描述	量化赋值
软件利用	攻击者可以通过执行软件代码触发漏洞	1
硬件利用	攻击者需要利用处理器芯片的物理接口或物理信息才能触发漏洞	0.5

6.2.1.2 攻击确定性

攻击确定性指实现攻击的确定性，描述处理器逻辑设计导致攻击的确定程度。

攻击确定性的赋值包括高、中、低，通常攻击确定性越高，漏洞危害程度越高。见表 2。

表 2 攻击确定性赋值说明表

赋值	描述	量化赋值
高	漏洞触发原理清楚，按照一定流程触发则攻击成功概率可达90%	1
中	漏洞触发原理清楚，但触发条件达到需要随机测试，测试成功概率可达50%以上	0.6
低	漏洞触发原理不清楚，或漏洞触发原理清楚，但触发条件达到需要随机测试，测试成功概率不足50%	0.2

6.2.1.3 权限需求

权限需求指触发漏洞所需的最低权限。

权限需求赋值包括无、低和高，通常权限需求越低，漏洞危害程度越高。见表 3。

表 3 权限需求赋值说明表

赋值	描述	量化赋值
无	不需要用户权限	1
低	普通用户权限	0.9
高	高级别用户权限	0.7

6.2.1.4 交互条件

交互条件是指漏洞触发是否需要攻击者之外的其他用户或系统配合、参与。

交互条件的赋值包括不需要、需要。通常不需要交互条件就能触发的漏洞危害较高。见表 4。

表 4 交互条件赋值说明表

赋值	描述	量化赋值
不需要	攻击过程中，不需要攻击者以外的其他用户或系统配合、参与	1
需要	攻击过程中，需要攻击者以外的其他用户或系统配合、参与	0.75

6.2.1.5 利用代码成熟度

利用代码成熟度反映攻击者是否可以获取可用的漏洞利用代码。

利用代码成熟度指标赋值包括高、中、低。通常利用代码成熟度越高，漏洞危害越大。见表 5。

表 5 利用代码成熟度赋值说明表

赋值	描述	量化赋值
高	具有成熟的漏洞利用代码，攻击者获得后可直接使用	1
中	攻击者可获取漏洞利用代码，但需要进行修改后才能够使用	0.9
低	不具备成熟的漏洞利用代码，需要攻击者自行开发	0.7

6.2.1.6 修复难度

修复难度反映处理器厂商或操作系统厂商对该漏洞进行修复的难度。

修复难度指标赋值包括高、中、低。通常修复难度越高，漏洞危害越大。见表 6。

表 6 补丁水平赋值说明表

赋值	描述	量化赋值
高	需要修改硬件才能彻底修复	1
中	通过微码更新即能彻底修复	0.9
低	通过软件修改即能彻底修复	0.7

6.2.2 影响程度

影响程度包含两部分，包括安全性影响和性能影响。安全性影响描述触发漏洞对处理器芯片安全性造成的损害程度。性能影响描述评价漏洞修复对性能的影响范围。

6.2.2.1 安全性影响

安全性影响范围由漏洞对处理器内部存储信息的机密性、完整性、可用性和权限正确性破坏程度决定。

机密性指标反映漏洞对处理器内部存储信息的机密性破坏程度。

完整性指标反映漏洞对处理器内部存储信息的完整性破坏程度。

可用性指标反映漏洞对处理器内部存储信息的可用性破坏程度。

权限正确性反映在漏洞利用过程中，对权限正确性的破坏程度。

机密性、完整性和可用性指标赋值均包括高、中、低、无。见表 7。

表 7 机密性、完整性、可用性指标赋值说明表

赋值	描述	量化赋值
高	严重影响处理器芯片存储的信息资源的安全属性，造成重大损失	0.56
中	中等程度影响处理器芯片存储的信息资源的安全属性，总体造成一定损失	0.35
低	低程度影响处理器芯片存储的信息资源的安全属性，但总体不会造成重大损失	0.21
无	不影响处理器芯片存储的信息资源对应的安全属性	0.07

权限正确性根据在攻击过程中，攻击者对处理器管理权限的最高破坏程度，分为9个级别。见表 8。

表 8 权限正确性赋值说明表

赋值	描述	量化赋值
0	无非法访问	0

1	同用户进程用户空间非法访问	0.2
2	单进程用户空间到内核空间非法访问	0.3
3	多用户进程间非法访问	0.5
4	VM客户机到VM内核非法访问	0.6
5	同一个物理机上两个客户机之间非法访问	0.75
6	非法获取获取Bios/SMM权限	0.8
7	非法获取可信执行环境权限	0.9
8	非法获取局域网另一台主机权限	1

6.2.2.2 性能影响

性能影响范围由修复漏洞对处理器性能损害程度决定。

性能影响赋值包括高、中、低，性能影响越高，表示该漏洞修复机率越小。见表 9。

表 9 性能影响赋值情况表

赋值	描述	量化赋值
高	修复该漏洞对性能造成重大影响	1
中	修复该漏洞对性能造成一定影响	0.6
低	修复该漏洞对性能造成影响较小	0.2

6.2.3 环境因素

环境因素主要用于综合评分，主要描述处理器芯片在该环境下的应用特点，用以在综合评分中调整漏洞各指标的权重。

6.2.3.1 被利用成本

被利用成本指标反映，在应用环境下，触发漏洞所需的成本。例如设备是否连接到互联网，安全防护是否充分等。

被利用成本指标赋值包括低、中、高。通常成本越低，漏洞修复的必要性越高。见表 10。

表 10 被利用成本指标赋值

赋值	描述	量化赋值
低	设备连接到互联网，安全防护简单，缺乏安全巡检机制	1

中	设备连接到互联网，安全防护充分，有较完善的安全巡检机制	0.6
高	设备未连接到互联网，安全防护充分，有完善的安全巡检机制	0.2

6.2.3.2 影响范围

影响范围指标反映触发漏洞对环境的影响。

影响范围指标赋值包括高、中、低、无，通常漏洞对环境影响越高，漏洞修复的必要性越高。见表11。

表 11 影响范围指标赋值

赋值	描述	量化赋值
高	触发漏洞会对系统、资产等造成严重影响。例如对环境中50%以上资产造成影响，或者受到影响的实体在环境中处于重要位置，有重要的作用	1
中	触发漏洞会对系统、资产等造成中等程度影响。例如对环境中的10%-50%资产造成影响，或者受到影响的实体在环境中处于比较重要位置，有比较重要的作用	0.7
低	触发漏洞会对系统、资产等造成轻微影响。例如对环境中的低于10%的资产造成影响，或者受到影响的实体在环境中处于不重要位置，不具有重要的作用	0.4
无	漏洞触发不会对系统、资产等造成任何资产损失	0.2

6.2.3.3 安全要求

安全要求指标反映该应用环境下对机密性、完整性和可用性的要求。默认情况下，三种安全属性重要性相同。但某些场景下，个别安全属性的重要性如果高于其他安全属性，即可通过调整安全要求的等级实现不同安全性重要性的区分。

安全要求包含机密性要求、完整性要求和可用性要求三项指标。每项指标赋值位于(0，1)区间，且三项指标赋值之和为1。

6.2.3.4 性能要求

性能要求指标反映该应用环境下，处理器运行性能和安全性的重要程度。

性能要求的指标赋值包括：高、中、低，见表 12。

表 12 性能要求指标赋值

赋值	描述	量化赋值
高	该环境对处理器芯片运行性能要求高，性能重要性远大于安全性	0.7

中	该环境对处理器芯片运行性能有中等程度要求，安全性与性能同等重要	0.5
低	该环境对处理器芯片运行性能有较低要求，安全重要性远大于性能	0.2

6.3 处理器芯片硬件漏洞分级方法

6.3.1 概述

通用处理器芯片硬件漏洞分级根据场景不同，分为危害分级和修复必要性分级两种分级方式。危害分级均包括超危、高危、中危和低危四个等级，见表 13。

表 13 处理器芯片漏洞危害分级赋值说明

赋值	描述
超危	漏洞可以非常容易对处理器芯片内存储的数据信息造成特别严重的危害。
高危	漏洞容易对处理器芯片内存储的数据信息造成特别严重的危害。
中危	漏洞可以对处理器芯片内存储的数据信息造成一般后果，或者比较困难对上述信息造成严重后果。
低危	漏洞可以对处理器芯片内存储的数据信息造成轻微后果，或者非常困难对上述信息造成严重后果。

修复必要性分级包括高、中、低三个等级，见表 14。

表 14 修复必要性分级赋值说明

赋值	描述
高	在当前环境下，漏洞修复必要性很高，应立即进行修复
中	在当前环境下，漏洞修复必要性中等，可择期进行修复
低	在当前环境下，漏洞修复必要性较低，可暂时不进行修复

6.3.2 漏洞分级步骤

漏洞危害分级过程包括最初的指标赋值、中间的指标评级和最后的分级计算三个步骤，其中，指标赋值是对具体漏洞对每个漏洞分级指标进行人工赋值;指标评级是根据指标赋值结果,分别对被利用性、影响范围和环境因素三个指标类进行评级。分级计算是根据指标评级计算产生危害分级和修复必要性分级结果。危害分级结果由被利用性和影响范围两个指标类计算产生，修复必要性分级由被利用性、影响范围和环境因素三个指标类计算产生。

6.3.3 危害等级指标评级

6.3.3.1 被利用性评级

被利用性评级反映处理器硬件漏洞触发的技术可能性。被利用性评分可根据指标组中各指标的量化评分进行计算。计算方法如下：

被利用性=攻击途径╳攻击确定性╳权限需求╳交互条件╳利用代码成熟度╳修复难度

根据被利用性的评分，对被利用性进行整体评级。评分与等级对应关系见表 15。

表 15 被利用性评级表

被利用性评分	被利用性等级
[0,0.15)	低
[0.15,0.4)	中
[0.4,0.8)	高
[0.8,1]	极高

6.3.3.2 影响程度评级

影响程度反映漏洞触发造成的后果。影响程度评分可根据指标组中各指标的量化评分进行计算。计算方法如下：

影响程度=（1-（1-机密性）╳（1-可用性）╳（1-完整性））╳权限正确性╳1.1

根据影响程度的评分，对影响程度进行整体评级。评分与等级对应关系见表 16。

表 16 影响范围评级表

影响程度评分	影响程度等级
[0,0.15)	低
[0.15,0.4)	中
[0.4,0.8)	高
[0.8,1]	极高

6.3.4 修复必要性等级指标评级

6.3.4.1 概述

修复必要性评级通过环境指标对被利用性和影响程度评级进行修正，根据修正后的被利用性和影响程度，计算最终的修复必要性等级。

6.3.4.2 修正被利用性评级

修正被利用性评级反映在环境因素影响下，处理器硬件漏洞触发的技术可能性。修正被利用性可根据被利用性和环境因素指标组中各指标的量化评分进行计算。计算方法如下：

修正被利用性=攻击途径╳攻击确定性╳权限需求╳交互条件╳利用代码成熟度╳修复难度╳被利用成本

根据修正被利用性的评分，对修正被利用性进行整体评级。评分与等级对应关系见表 17。

表 17 修正被利用性评级表

修正被利用性评分	修正被利用性评级
[0,0.15)	低
[0.15,0.4)	中
[0.4,0.8)	高
[0.8,1]	极高

6.3.4.3 修正影响程度评级

修正影响范围反映漏洞触发造成的后果。修正影响范围可根据影响范围和环境因素指标组中各指标的量化评分进行计算。计算方法如下：

影响程度=（机密性要求╳机密性+完整性要求╳完整性+可用性要求╳可用性）╳权限正确性╳影响范围-性能要求╳性能影响

根据修正影响范围的评分，对修正影响范围进行整体评级。评分与等级对应关系见表 18表 16。

表 18 修正影响程度评级

修正影响程度评分	修正影响程度评级
[0,0.15)	低
[0.15,0.4)	中
[0.4,0.8)	高
[0.8,1]	极高

6.3.5 漏洞分级

漏洞危害分级结果由被利用性和影响程度两个指标类决定。被利用性评级越高、影响程度评级越高，漏洞危害分级越高。漏洞分级方法如下：

首先，对被利用性和影响程度的指标进行量化赋值，然后参照前述指标评级步骤，计算得到被利用性和影响程度的评级。根据被利用性和影响程度评级结果，计算得到漏洞危害分级，见表 19。

表 19 漏洞危害评级表

		影响程度			
		低	中	高	极高
可利用性	低	低危	低危	低危	中危
	中	低危	中危	中危	高危
	高	低危	中危	高危	高危
	极高	中危	高危	高危	超危

6.3.6 漏洞修复必要性分级

漏洞修复必要性分级结果由环境因素修正的被利用性和影响程度两个指标类决定。被利用性评级越高、影响程度评级越高，漏洞修复必要性分级越高。漏洞分级方法如下：

首先，对被利用性、影响程度和环境因素的指标进行量化赋值，然后参照前述指标评级步骤，计算得到修正被利用性和修正影响程度的评级。根据修正被利用性和修正影响程度评级结果，见表 20。

表 20 漏洞修复必要性分级评级表

		修正影响程度			
		低	**中**	**高**	**极高**
修正可利用性	**低**	低	低	低	中
	中	低	低	中	中
	高	低	中	中	高
	极高	中	中	高	极高

•

——

附 录 A
（资料性）
处理器硬件漏洞评分示例

A.1 骑士漏洞评分示例

A.1.1 漏洞分级指标赋值

分级指标		赋值	量化赋值
被利用性	攻击途径	软件利用	1
	攻击确定性	高	1
	权限需求	高	0.7
	交互条件	不需要	1
	利用代码成熟度	低	0.7
	修复难度	高	1
影响程度	机密性	中	0.35
	完整性	中	0.35
	可用性	中	0.35
	权限正确性	跨安全区	0.9

A.1.2 漏洞指标评级

被利用性评级=1*1*0.7*1*0.7*1=0.49，评级为高。
影响程度评级=（1-（1-0.35）*（1-0.35）*（1-0.35））*0.9*1.1=0.71，评级为高。

A.1.3 漏洞危害分级

根据漏洞危害评级表，骑士漏洞总体评级为高危漏洞。

参 考 文 献

[1] Common Vulnerability Scoring System v3.0: Specification Document. https://www.first.org/cvss/v3.0/specification-document

[2] Radack, S. (2007), The Common Vulnerability Scoring System (CVSS), ITL Bulletin, National Institute of Standards and Technology, Gaithersburg, MD, [online], https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=51280 (Accessed August 2, 2024)