CGSL 系统开源组件 CVE 漏洞评估定级差异申明

CGSL 系统安全等级

CGSL 产品安全团队采用四分制（低、中、重要和严重）以及通过安全漏洞评分系统（CVSS）基础得分，为在 CGSL 系列系统中找到的安全问题进行分级。这些方法提供了指定有限顺序的风险评估，以帮忙您了解并安排系统升级，并可让您对独特环境中的每个问题的风险作出知情决策。

四分制分级方法让您了解 CGSL 对问题的重视程度，并帮助您判断问题严重性以及确定最重要的更新是什么。这个分级方法根据对确切缺陷及其类型的技术分析后来考虑潜在风险，而不是当前威胁程度；如果后续出现针对此漏洞的攻击或蠕虫，或者在发布修复方案前已有解决方案，则给出的评级不会改变。

	严重性分级	描述
	Critical 影响	这个分级用于可被远程非授权攻击者轻易攻击的漏洞，并可造成没有用户互动情况下的系统破解（随机代码执行）。这些类型的漏洞可被蠕虫攻击。需要授权远程用户、本地用户或不太可能的配置的漏洞不属于 Critical 影响等级。
	Important 影响	这个分级用于可轻易破解资源机密性、完整性及可用性的漏洞。这些类型的漏洞可让本地用户获得特权，让非验证的远程用户查看使用验证保护的资源，让验证的远程用户执行随机代码，或允许远程用户造成服务拒绝。
	Moderate 影响	这个分级用于攻击比较困难，但在某些条件下仍可对资源机密性、完整性或可用性造成一定损害的漏洞。这些漏洞类型可能会造成 Critical 影响或 Important 影响，但根据对漏洞的技术，对该漏洞的攻击并不容易，或只能影响不太可能的配置。
	Low 影响	这个分级用于有安全影响的所有其他问题。这些漏洞类型只有在不太可能的情况下方可进行攻击，或成功的攻击造成的后果并不严重。

通用漏洞评分系统（CVSS）

通用漏洞评分系统（CVSS）基础得分提供有关某个漏洞的附加指导，通过为漏洞的恒定方面评分给出详细的严重性等级：这些常量方面为访问向量、访问复杂性、验证、机密性、完常量及可用性。

漏洞严重性评估

业界普遍使用 CVSS 标准评估漏洞的严重性，CGSL 在使用 CVSSv3 进行漏洞评估时，需要设定漏洞共计场景，基于在该攻击场景下的实际影响进行评估。漏洞严重性等级评估是指针对漏洞利用难易程度，以及利用后对机密性、完整性、可用性的影响进行评估，并生成一个评分值。

CVSS v3 基本衡量标准

CVSS v3 基本衡量标准是通过对如下常量来评估一个漏洞的影响：

- 攻击平台（Attack Vector，AV） - 表示攻击的“远程性”以及如何利用此漏洞。
- 攻击复杂性（Attack Complexity，AC） - 说明执行攻击的难度以及成功进行攻击所需的因素。
- 用户互动（User Interaction，UI） - 确定该攻击是需要人为的参与，还是可以自动完成。
- 特权要求（Privileges Required，PR） - 说明攻击成功所要求的用户验证等级。
- 范围（Scope，S） - 确定攻击者是否可以影响具有不同授权等级的组件。
- 机密性（Confidentiality，C） - 确定是否将数据披露给未授权方后导致的影响程度。
- 完整性（Integrity，I） - 这个常量评估数据的可信度以及在什么情况下可以不被非授权用户修改。
- 可用性（Availability，A） - 衡量用户在需要访问数据或服务时受影响的程度。

NVD 与 CGSL 系统评估分数差异说明

针对各供应商提供的开源软件，CVSS 的基础评分会因为各 Linux 供应商的版本而定；具体取决于提供的版本，使用的方式、平台以及软件的编译方式。

NVD 的评分考虑了漏洞被利用的所有场景，而 CGSL 系统是基于开源社区自行构建，主要用于服务器场景，所以对于 CGSL 系列产品来说，直接采用 NVD 评分是不合适的，因此，CGSL 系统对所有受影响的 CVE 有自己的评分，存在评估分数与 NVD 不同的情况。