【CVE-2023-23583】Intel 解决高严重性 CPU 漏洞 (https://md5ol.com/260/)

2023-11-15 18:06 | 33 | 0 |
新闻 (https://md5ol.com/category/%e6%96%b0%e9%97%bb/),漏洞 (https://md5ol.com/category/%e6%bc%8f%e6%b4%9e/)
546 字 | 3 分钟

英特尔已解决 (https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00950.html)一个高严重性漏洞，影响其现代桌面、服务器、移动和嵌入式 CPU，包括最新的 Alder Lake、Raptor Lake 和 Sapphire Rapids 微架构。该漏洞被跟踪为 CVE-2023-23583，CVSS 评分为 8.8，可能允许具有本地访问权限的攻击者升级权限、访问敏感信息或触发拒绝服务 (DoS) 条件。

该漏洞源于 Intel CPU 解释冗余指令前缀的方式中的缺陷。攻击者可以利用此缺陷绕过安全边界并在受影响的系统上执行任意代码。这可能使他们能够控制系统、窃取敏感数据或扰乱运营。

该漏洞影响了多种英特尔CPU，包括 (https://www.intel.com/content/www/us/en/developer/articles/technical/software-security-guidance/advisory-guidance/redundant-prefix-issue.html):

- lder Lake
- Raptor Lake
- Sapphire Rapids
- Ice Lake
- Tiger Lake
- Rocket Lake
- Comet Lake
- Kaby Lake
- Skylake
- Broadwell

- Haswell

英特尔已发布微代码更新来解决该漏洞。建议用户更新其 BIOS、系统操作系统和驱动程序，以便从原始设备制造商 (OEM)、操作系统供应商 (OSV) 和虚拟机管理程序供应商接收最新的微代码。

这个案例特别有趣的是漏洞的双重发现。英特尔的研究人员在审查即将发布的功能勘误表时发现了“冗余前缀”。在并行开发中，谷歌研究人员独立发现了相同的拒绝服务缺陷。

谷歌将该漏洞称为 Reptar (CVE-2023-23583)，并详细说明该问题是由 CPU 解释冗余指令前缀的方式引起的。这种误解可能会导致安全边界被绕过。谷歌也发布了 (https://lock.cmpxchg8b.com/reptar.html)有关漏洞的详细报告，其中提供了有关技术细节和潜在影响的附加信息。

Reptar 漏洞是一个严重的安全问题，攻击者可利用该漏洞对受影响的系统进行未经授权的访问。用户需要尽快应用可用的补丁，以降低被利用的风险。

CVE-2023-23583 (https://md5ol.com/tag/cve-2023-23583/)

暂无评论

上一篇

【CVE-2023-47359】VLC 媒体播放器缓冲区溢出漏洞

下一篇

【CVE-2023-34060】VMware Cloud Director 设备中未修补的严重缺陷

推荐文章

【CVE-2023-46302】严重的 Apache Submarin...

【CVE-2023-46214】Splunk 远程命令执行利用脚本...

【CVE-2023-4357】Chrome-XXE POC概念验证

【CVE-2023-47246】SysAid RCE（shell 上传）利用...

【CVE-2023-48365】严重的 Qlik Sense Enterprise ...