PSIRT Notification

C2000 DCSM ROM 代码片段/ROP 漏洞

总结

攻击者可能利用多个基于 C2000 C28 的产品中的安全 ROM 实现，绕过双代码安全模式 (DCSM) 强制的存储器区域保护。可能会绕过 DCSM 保护的最内部边界，对安全存储器区域进行攻击。

漏洞

TI PSIRT ID

TI-PSIRT-2023-080189

定义

- **代码片段：**攻击者以原始程序未预期的方式恶意使用存储器中存在的指令序列。代码片段通常链接在一起，作为一个简单的单元执行满足攻击者目的的任意计算或函数。
- **ROP：**面向返回的编程；一种通过修改栈存储器的返回地址位置将代码片段连接在一起的攻击方法。
- **PSIRT：**TI 的产品安全事件响应团队负责监督接受和响应涉及 TI 半导体产品（包括硬件、软件和文档）潜在安全漏洞报告的流程。如需更多信息，请参见 TI PSIRT。
- **CVSS：**常见的漏洞评分系统，由 FIRST 维护。

CVE ID

不适用。

CVSS 基础分数

6.7

CVSS 矢量

CVSS:3.1/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N

受影响的产品

- TMS320F28003x
- TMS320F2838x
- TMS320F280013x
- TMS320F280015x
- TMS320F28P65x

可能受影响的功能

以下属性可能会受到此漏洞的影响：

- 存储器中 EXEONLY 代码的机密性和完整性。
- 存储器中非 EXEONLY 数据/代码的机密性和完整性。

建议的缓解措施

启用器件上现有的两个功能：

- **JTAGLOCK**。JTAG 接口应该被锁定。有关如何锁定 JTAG 接口，请参阅 SPRACS4 应用报告。
- **零引脚引导至闪存引导方法**。引导方法应编程为始终直接引导到内部闪存引导模式，即“闪存”或“安全闪存”。有关如何启用的详细信息，请参阅器件的技术参考手册。

这两个特性可防止攻击者连接调试程序或使用引导加载程序将代码加载到内部存储器。在安全存储器区域启动 ROP/代码片段攻击时，需要这种注入的代码。还应该对用户应用程序代码采用网络安全编码和测试最佳实践，以防止攻击者将其代码加载到内部存储器中。这包括但不限于次级引导加载程序、固件更新代码以及通信栈。

鸣谢

感谢 Cyberpeace Tech Co., Ltd. 的 Zhao Hai 向 TI 产品安全事件响应团队 (PSIRT) 报告此漏洞。

修订历史记录

注：以前版本的页码可能与当前版本的页码不同

日期	修订版本	说明
November 2023	*	初始发行版

重要声明和免责声明

TI“按原样”提供技术和可靠性数据（包括数据表）、设计资源（包括参考设计）、应用或其他设计建议、网络工具、安全信息和其他资源，不保证没有瑕疵且不做出任何明示或暗示的担保，包括但不限于对适销性、某特定用途方面的适用性或不侵犯任何第三方知识产权的暗示担保。

这些资源可供使用 TI 产品进行设计的熟练开发人员使用。您将自行承担以下全部责任：(1) 针对您的应用选择合适的 TI 产品，(2) 设计、验证并测试您的应用，(3) 确保您的应用满足相应标准以及任何其他功能安全、信息安全、监管或其他要求。

这些资源如有变更，恕不另行通知。TI 授权您仅可将这些资源用于研发本资源所述的 TI 产品的应用。严禁对这些资源进行其他复制或展示。您无权使用任何其他 TI 知识产权或任何第三方知识产权。您应全额赔偿因在这些资源的使用中对 TI 及其代表造成的任何索赔、损害、成本、损失和债务，TI 对此概不负责。

TI 提供的产品受 TI 的销售条款或 ti.com 上其他适用条款/TI 产品随附的其他适用条款的约束。TI 提供这些资源并不会扩展或以其他方式更改 TI 针对 TI 产品发布的适用的担保或担保免责声明。

TI 反对并拒绝您可能提出的任何其他或不同的条款。

邮寄地址：Texas Instruments, Post Office Box 655303, Dallas, Texas 75265