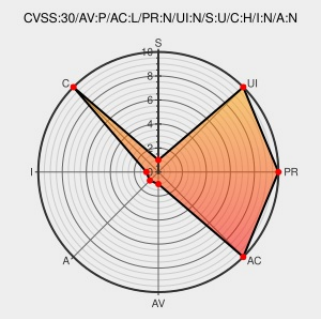
CVE-2018-18056

Published on: 08/20/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:52 PM UTC

CVE-2018-18056

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Tm4c123 from Ti contain the following vulnerability:

An issue was discovered in the Texas Instruments (TI) TM4C, MSP432E and MSP432P microcontroller series. The eXecute-Only-Memory (XOM) implementation prevents code read-outs on protected memory by generating bus faults. However, single-stepping and using breakpoints is allowed in XOM-protected flash memory. As a consequence, it is possible to execute single instructions with arbitrary system states (e.g., registers, status flags, and SRAM content) and observe the state changes produced by the unknown instruction. An attacker could exploit this vulnerability by executing protected and unknown instructions with specific system states and observing the state changes. Based on the gathered information, it is possible to reverse-engineer the executed instructions. The processor acts as a kind of "instruction oracle."

CVE-2018-18056 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 4.6 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
PHYSICAL	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	NONE	NONE

CVSS2 Score: 2.1 - LOW

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
Taking a Look into Execute-Only Memory | USENIX	Technical Description Third Party Advisory www.usenix.org text/html	MISC www.usenix.org/conference/woot19/presentation/schink
	Technical Description Third Party Advisory www.usenix.org application/pdf	MISC www.usenix.org/system/files/woot19-paper_schink.pdf

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Ti	Tm4c123	-	All	All	All
Hardware	Ti	Tm4c123	-	All	All	All
Operating System	Ti	Tm4c123 Firmware	-	All	All	All
Operating System	Ti	Tm4c123 Firmware	-	All	All	All
Hardware	Ti	Tm4c129	-	All	All	All
Hardware	Ti	Tm4c129	-	All	All	All
Operating System	Ti	Tm4c129 Firmware	-	All	All	All
Operating System	Ti	Tm4c129 Firmware	-	All	All	All

cpe:2.3:h:ti:tm4c123:-:*:*:*:*:*:*:*:

cpe:2.3:h:ti:tm4c123:-:*:*:*:*:*:*:*:

cpe:2.3:o:ti:tm4c123_firmware:-:*:*:*:*:*:*:*:

cpe:2.3:o:ti:tm4c123_firmware:-:*:*:*:*:*:*:*:

cpe:2.3:h:ti:tm4c129:-:*:*:*:*:*:*:*:

cpe:2.3:h:ti:tm4c129:-:*:*:*:*:*:*:*:

cpe:2.3:o:ti:tm4c129_firmware:-:*:*:*:*:*:*:*:

cpe:2.3:o:ti:tm4c129_firmware:-:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report