

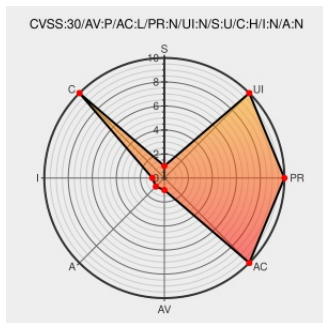


CVE-2018-18056

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 [M](#) 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

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

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](#) 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)