

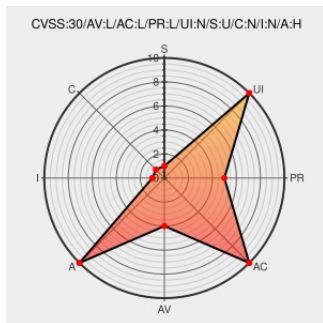


CVE-2017-5699

Published on: 01/17/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:47 PM UTC

CVE-2017-5699

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Minnowboard 3](#) from [Intel](#) contain the following vulnerability:

Input validation error in Intel MinnowBoard 3 Firmware versions prior to 0.65 allow local attacker to cause denial of service via UEFI APIs.

CVE-2017-5699 has been assigned by [intel](#) [secure@intel.com](#) to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [intel](#) **Intel Corporation** - **MinnowBoard 3** version **before 0.65**

CVSS3 Score: **5.5 - MEDIUM**

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

CVSS2 Score: **2.1 - LOW**

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

CVE References

Description	Tags	Link
27. UEFI Variable Deletion/Corruption - Security Advisory	Patch Third Party Advisory edk2-docs.gitbooks.io	CONFIRM edk2-docs.gitbooks.io/security-advisory/content/uefi-variable-deletioncorruption.html

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 	Intel	Minnowboard 3	-	All	All	All
Hardware 	Intel	Minnowboard 3	-	All	All	All
Operating System	Intel	Minnowboard 3 Firmware	All	All	All	All
Operating System	Intel	Minnowboard 3 Firmware	All	All	All	All
cpe:2.3:h:intel:minnowboard_3:-:~::~~::~~::~~::~~::~~::~~::~::						
cpe:2.3:h:intel:minnowboard_3:-:~::~~::~~::~~::~~::~~::~~::~::						
cpe:2.3:o:intel:minnowboard_3_firmware:~::~~::~~::~~::~~::~~::~~::~::						
cpe:2.3:o:intel:minnowboard_3_firmware:~::~~::~~::~~::~~::~~::~~::~::						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

Next ID→