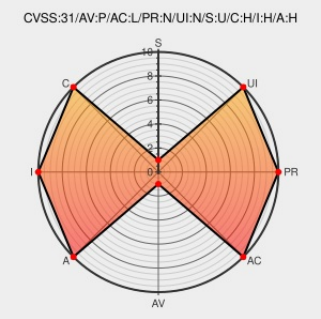
CVE-2014-4860

Published on: 01/31/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:45 PM UTC

CVE-2014-4860

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



Certain versions of Edk2 from Tianocore contain the following vulnerability:

Multiple integer overflows in the Pre-EFI Initialization (PEI) boot phase in the Capsule Update feature in the UEFI implementation in EDK2 allow physically proximate attackers to bypass intended access restrictions by providing crafted data that is not properly handled during the coalescing phase.

CVE-2014-4860 has been assigned by cert@cert.org to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **Phoenix Technologies Ltd.** - **SCT3** version **before 5/23/2014**

Affected Vendor/Software: **American Megatrends Incorporated (AMI)** - **BIOS** version **unknown**

CVSS3 Score: 6.8 - MEDIUM

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

CVSS2 Score: 7.2 - HIGH

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

CVE References

Description	Tags	Link

Description	Tags	Link
Vulnerability Note VU#552286 - UEFI EDK2 Capsule Update vulnerabilities	Third Party Advisory US Government Resource www.kb.cert.org text/html	MISC www.kb.cert.org/vuls/id/552286

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
Application	Tianocore	Edk2	-	All	All	All
Application	Tianocore	Edk2	-	All	All	All

cpe:2.3:a:tianocore:edk2:-:*:*:*:*:*:*:*:

cpe:2.3:a:tianocore:edk2:-:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→