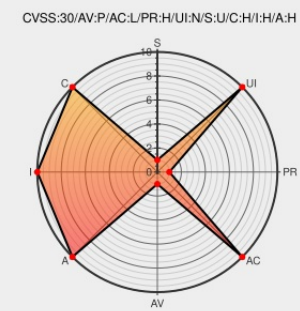
CVE-2018-12199

Published on: 03/14/2019 12:00:00 AM UTC

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

CVE-2018-12199

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



Certain versions of Converged Security Management Engine Firmware from Intel contain the following vulnerability:

Buffer overflow in an OS component in Intel CSME before versions 11.8.60, 11.11.60, 11.22.60 or 12.0.20 and Intel TXE version before 3.1.60 or 4.0.10 may allow a privileged user to potentially execute arbitrary code via physical access.

CVE-2018-12199 has been assigned by intel secure@intel.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: intel **Intel Corporation** - **Intel(R) CSME, Server Platform Services, Trusted Execution Engine and Intel(R) Active Management Technology** version **Multiple versions.**

CVSS3 Score: 6.2 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
PHYSICAL	LOW	HIGH	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
INTEL-SA-00185	Vendor Advisory www.intel.com	intel CONFIRM www.intel.com/content/www/us/en/security-

	text/html	center/advisory/INTEL-SA-00185.html
Intel SA-00185 CSME-SPS-TXE-AMT Vulnerabilities in NetApp Products | NetApp Product Security	Third Party Advisory security.netapp.com text/html	CONFIRM security.netapp.com/advisory/ntap-20190318-0001/

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
Operating System	Intel	Converged Security Management Engine Firmware	All	All	All	All
Operating System	Intel	Converged Security Management Engine Firmware	All	All	All	All
Operating System	Intel	Trusted Execution Engine Firmware	All	All	All	All
Operating System	Intel	Trusted Execution Engine Firmware	All	All	All	All

cpe:2.3:o:intel:converged_security_management_engine_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:o:intel:converged_security_management_engine_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:o:intel:trusted_execution_engine_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:o:intel:trusted_execution_engine_firmware:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→