



# CVE-2020-12355

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2020-12355
<b>State</b>	PUBLIC
<b>Assigner</b>	secure@intel.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-11-12 18:15:00 UTC
<b>Updated</b>	2020-11-24 20:51:00 UTC
<b>Description</b>	Authentication bypass by capture-replay in RPMB protocol message authentication subsystem in Intel(R) TXE versions before

## Risk And Classification

**Problem Types:** CWE-294

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Intel</a>	<a href="#">Trusted Execution Engine</a>	All	All	All	All
Operating System	<a href="#">Intel</a>	<a href="#">Trusted Execution Engine</a>	All	All	All	All

## References

Reference	Source	Link	Tags
Intel SA-00391 Intel TXE Vulnerabilities in NetApp Products   NetApp Product Security	CONFIRM	<a href="https://security.netapp.com">security.netapp.com</a>	Third Party Advis
INTEL-SA-00391	MISC	<a href="https://www.intel.com">www.intel.com</a>	Vendor Advisory
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, analy

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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](#)**