



# CVE-2021-25252

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

## Summary

<b>CVE</b>	CVE-2021-25252
<b>State</b>	PUBLIC
<b>Assigner</b>	security@trendmicro.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-03-03 16:15:00 UTC
<b>Updated</b>	2021-09-08 17:23:00 UTC
<b>Description</b>	Trend Micro's Virus Scan API (VSAPI) and Advanced Threat Scan Engine (ATSE) - are vulnerable to a memory exhaustion

## Risk And Classification

**Problem Types:** CWE-400

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Apple</a>	<a href="#">Macos</a>	-	All	All	All
Operating System	<a href="#">Apple</a>	<a href="#">Mac Os</a>	-	All	All	All
Hardware	<a href="#">Emc</a>	<a href="#">Celerra Network Attached Storage</a>	-	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	-	All	All	All
Operating System	<a href="#">Microsoft</a>	<a href="#">Windows</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">Cluster Data Ontap</a>	-	All	All	All
Operating System	<a href="#">Novell</a>	<a href="#">Netware</a>	-	All	All	All
Application	<a href="#">Trendmicro</a>	<a href="#">Apex Central</a>	2019	-	All	All
Application	<a href="#">Trendmicro</a>	<a href="#">Apex One</a>	-	-	All	All
Application	<a href="#">Trendmicro</a>	<a href="#">Apex One</a>	2019	-	All	All
Application	<a href="#">Trendmicro</a>	<a href="#">Cloud Edge</a>	5.0	All	All	All
Application	<a href="#">Trendmicro</a>	<a href="#">Control Manager</a>	7.0	-	All	All
Application	<a href="#">Trendmicro</a>	<a href="#">Deep Discovery Analyzer</a>	5.1	-	All	All
Application	<a href="#">Trendmicro</a>	<a href="#">Deep Discovery Email Inspector</a>	2.5	-	All	All
Application	<a href="#">Trendmicro</a>	<a href="#">Deep Discovery Inspector</a>	3.8	-	All	All
Application	<a href="#">Trendmicro</a>	<a href="#">Deep Security</a>	10.0	-	All	All
Application	<a href="#">Trendmicro</a>	<a href="#">Deep Security</a>	11.0	-	All	All

Application	Trendmicro	Deep Security	12.0	-	All	All
Application	Trendmicro	Deep Security	20.0	-	All	All
Application	Trendmicro	Interscan Messaging Security Virtual Appliance	9.1	-	All	All
Application	Trendmicro	Interscan Web Security Virtual Appliance	6.5	-	All	All
Application	Trendmicro	Officescan	-	All	All	All
Application	Trendmicro	Portal Protect	2.6	All	All	All
Application	Trendmicro	Safe Lock	1.1	-	All	All
Application	Trendmicro	Scanmail	14.0	All	All	All
Application	Trendmicro	Scanmail For Exchange	14.0	-	All	All
Application	Trendmicro	Scanmail For Ibm Domino	5.8	-	All	All
Application	Trendmicro	Serverprotect	5.8	-	All	All
Application	Trendmicro	Serverprotect For Network Appliance Filers	5.8	-	All	All
Application	Trendmicro	Serverprotect For Storage	6.0	-	All	All
Application	Trendmicro	Worry-free Business Security	10.1	-	All	All

## References

Reference	Source	Link
SECURITY BULLETIN: Trend Micro Scan Engine Memory Exhaustion Denial-of-Service Vulnerability	MISC	<a href="https://success.trendmicro.com">success.trendmicro.com</a>
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

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

© CVE.report 2026 |

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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/cve).

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)