



# CVE-2020-8607

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

## Summary

<b>CVE</b>	CVE-2020-8607
<b>State</b>	PUBLIC
<b>Assigner</b>	security@trendmicro.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-08-05 14:15:00 UTC
<b>Updated</b>	2020-08-11 15:02:00 UTC
<b>Description</b>	An input validation vulnerability found in multiple Trend Micro products utilizing a particular version of a specific rootkit prote

## Risk And Classification

### Problem Types: CWE-20

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Microsoft	Windows	-	All	All	All
Operating System	Microsoft	Windows	-	All	All	All
Application	Trendmicro	Antivirus Toolkit	All	All	All	All
Application	Trendmicro	Antivirus Toolkit	All	All	All	All
Application	Trendmicro	Apex One	2019	All	All	All
Application	Trendmicro	Apex One	saas	All	All	All
Application	Trendmicro	Apex One	2019	All	All	All
Application	Trendmicro	Apex One	saas	All	All	All
Application	Trendmicro	Deep Security	10.0	All	All	All
Application	Trendmicro	Deep Security	11.0	All	All	All
Application	Trendmicro	Deep Security	12.0	All	All	All
Application	Trendmicro	Deep Security	9.6	All	All	All
Application	Trendmicro	Deep Security	10.0	All	All	All
Application	Trendmicro	Deep Security	11.0	All	All	All
Application	Trendmicro	Deep Security	12.0	All	All	All
Application	Trendmicro	Deep Security	9.6	All	All	All
Application	Trendmicro	Officescan	xg	sp1	All	All

Application	Trendmicro	Officescan	xg	sp1	All	All
Application	Trendmicro	Officescan Business Security	10.0	sp1	All	All
Application	Trendmicro	Officescan Business Security	9.0	All	All	All
Application	Trendmicro	Officescan Business Security	9.5	All	All	All
Application	Trendmicro	Officescan Business Security	10.0	sp1	All	All
Application	Trendmicro	Officescan Business Security	9.0	All	All	All
Application	Trendmicro	Officescan Business Security	9.5	All	All	All
Application	Trendmicro	Officescan Business Security Service	-	All	All	All
Application	Trendmicro	Officescan Business Security Service	-	All	All	All
Application	Trendmicro	Officescan Cloud	15	All	All	All
Application	Trendmicro	Officescan Cloud	16.0	All	All	All
Application	Trendmicro	Officescan Cloud	15	All	All	All
Application	Trendmicro	Officescan Cloud	16.0	All	All	All
Application	Trendmicro	Online Scan	8.0	All	All	All
Application	Trendmicro	Online Scan	8.0	All	All	All
Application	Trendmicro	Portable Security	2.0	All	All	All
Application	Trendmicro	Portable Security	3.0	All	All	All
Application	Trendmicro	Portable Security	2.0	All	All	All
Application	Trendmicro	Portable Security	3.0	All	All	All
Application	Trendmicro	Rootkit Buster	2.2	All	All	All
Application	Trendmicro	Rootkit Buster	2.2	All	All	All
Application	Trendmicro	Safe Lock	-	All	All	All
Application	Trendmicro	Safe Lock	2.0	sp1	All	All
Application	Trendmicro	Safe Lock	-	All	All	All
Application	Trendmicro	Safe Lock	2.0	sp1	All	All
Application	Trendmicro	Serverprotect	5.8	All	All	All
Application	Trendmicro	Serverprotect	5.8	All	All	All
Application	Trendmicro	Serverprotect	5.8	All	All	All
Application	Trendmicro	Serverprotect	6.0	All	All	All
Application	Trendmicro	Serverprotect	5.8	All	All	All
Application	Trendmicro	Serverprotect	5.8	All	All	All
Application	Trendmicro	Serverprotect	5.8	All	All	All
Application	Trendmicro	Serverprotect	6.0	All	All	All

## References

Reference	Source	Link
SECURITY BULLETIN: Input Validation Vulnerability in Trend Micro Rootkit Driver (Multiple Products)	N/A	<a href="https://success.trendmicro.com">success.trendmicro.com</a>
JVNVU#99160193: Trend Micro anti-rootkit driver improperly validates inputs	N/A	<a href="https://jvn.jp">jvn.jp</a>
Q&A   Trend Micro Business Support	N/A	<a href="https://success.trendmicro.com">success.trendmicro.com</a>
JVNVU#99160193:トレンドマイクロ社のルートキット対策ドライバに入力値検証不備の脆弱性	N/A	<a href="https://jvn.jp">jvn.jp</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](https://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.cve.org). This site includes MITRE data granted under the following [license](https://www.mitre.org/licenses/mitre).

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