



CVE-2018-18328

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

Summary

CVE	CVE-2018-18328
State	PUBLIC
Assigner	security@trendmicro.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-10-23 14:29:00 UTC
Updated	2018-12-04 13:22:00 UTC
Description	A KERedirect Untrusted Pointer Dereference Privilege Escalation vulnerability in Trend Micro Antivirus for Mac (Consumer)

Risk And Classification

Problem Types: CWE-476

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Trendmicro	Antivirus For Mac 2017	All	All	All	All
Application	Trendmicro	Antivirus For Mac 2018	All	All	All	All
Application	Trendmicro	Antivirus For Mac 2019	All	All	All	All

References

Reference	Source	Link	Tags
ZDI-18-1296 Zero Day Initiative	MISC	www.zerodayinitiative.com	Third Party Advisory, VDB Entry
esupport.trendmicro.com/solution/ja-jp/1121350.aspx	CONFIRM	esupport.trendmicro.com	Vendor Advisory
Home · Trend Micro for Home	CONFIRM	esupport.trendmicro.com	Vendor Advisory
Malformed Request	BID	www.securityfocus.com	Third Party Advisory, VDB Entry
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

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](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)