



CVE-2020-28576

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

Summary

CVE	CVE-2020-28576
State	PUBLIC
Assigner	security@trendmicro.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-12-01 19:15:00 UTC
Updated	2021-07-21 11:39:00 UTC
Description	An improper access control information disclosure vulnerability in Trend Micro Apex One and OfficeScan XG SP1 could allow an attacker to access sensitive information.

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Trendmicro	Apex One	2019	All	All	All
Application	Trendmicro	Apex One	2019	All	All	All
Application	Trendmicro	Officescan	xg	sp1	All	All
Application	Trendmicro	Officescan	xg	sp1	All	All

References

Reference	Source	Link
SECURITY BULLETIN: November 2020 Security Bulletin for Trend Micro Apex One and Apex One as a Service	MISC	success.trendmicro.com
ZDI-20-1375 Zero Day Initiative	MISC	www.zerodayinitiative.com
SECURITY BULLETIN: November 2020 Security Bulletin for Trend Micro OfficeScan XG SP1	MISC	success.trendmicro.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

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](#)