



CVE-2020-24562

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

Summary

CVE	CVE-2020-24562
State	PUBLIC
Assigner	security@trendmicro.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-09-29 00:15:00 UTC
Updated	2021-07-21 11:39:00 UTC
Description	A vulnerability in Trend Micro OfficeScan XG SP1 on Microsoft Windows may allow an attacker to create a hard link to any

Risk And Classification

Problem Types: CWE-59

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	Officescan	xg	sp1	All	All
Application	Trendmicro	Officescan	xg	sp1	All	All

References

Reference	Source	Link	T
SECURITY BULLETIN: Trend Micro OfficeScan XG Hard Link Privilege Escalation Vulnerability	N/A	success.trendmicro.com	V
ZDI-20-1226 Zero Day Initiative	N/A	www.zerodayinitiative.com	T
CVE Program record	CVE.ORG	www.cve.org	c
NVD vulnerability detail	NVD	nvd.nist.gov	c

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[375757](#) Trend Micro Apex One(On-Prem) Multiple Vulnerabilities(000263632)(August 2020)

[375758](#) Trend Micro OfficeScan XG Hard Link Privilege Escalation Vulnerability(000263632)

© [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](#)