

CVE-2021-36741

Trend Micro Multiple Products Improper Input Validation Vulnerability

CISA KEV since Nov 3, 2021

Actively exploited

An improper input validation vulnerability in Trend Micro Apex One, Apex One as a Service, OfficeScan XG, and Worry-Free Business Security 10.0 SP1 allows a remote attacker to upload arbitrary files on affected installations. Please note: an attacker must first obtain the ability to logon to the product's management console in order to exploit this vulnerability.

EVRS 75 _{/100} Urgent priority	CVSS V3.1 8.8 High · NVD	EPSS 0.050 92.1st percentile · FIRST	CISA DEADLINE Nov 17, 2021 KEV since 2021 · listed over a year
--	--	--	--

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.050 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 8.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: Apply updates per vendor instructions.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
officescan	xg	no fixed version listed	NVD
officescan business security	10.0	no fixed version listed	NVD
apex one	2019	no fixed version listed	NVD
worry-free business security	10.0	no fixed version listed	NVD
windows	—	no fixed version listed	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-7w3v-7x22-4g8v	Additional guidance	success.trendmicro.com/jp/solution/000287796
success.trendmicro.com	success.trendmicro.com/dcx/s/solution/000287819?language=en_US , https://success.trendmicro.com/dcx/s/solution/000287820?language=en_US	NVD	nvd.nist.gov/vuln/detail/CVE-2021-36741
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2021-23331
Current data	evulnable.com/vulnerability-management/cve/CVE-2021-36741		

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.