



CVE-2020-8467

Published on: 03/17/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:59 PM UTC

CVE-2020-8467

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Apex One](#) from [Trendmicro](#) contain the following vulnerability:

A migration tool component of Trend Micro Apex One (2019) and OfficeScan XG contains a vulnerability which could allow remote attackers to execute arbitrary code on affected installations (RCE). An attempted attack requires user authentication.

CVE-2020-8467 has been assigned by security@trendmicro.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: **Trend Micro - Trend Micro OfficeScan, Trend Micro Apex One version OfficeScan XG (12.0), Apex One 2019 (14.0)**

CVSS3 Score: **8.8 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **6.5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Q&A Trend Micro Business Support	Patch Vendor Advisory	MISC success.trendmicro.com/in/solution/000244253

text/html

success.trendmicro.com/solution/000245571

There are currently no QIDs associated with this CVE

```
cpe:2.3:a:trendmicro:officescan:xg:sp1:*:*:*:*:*:
```

Next ID→

