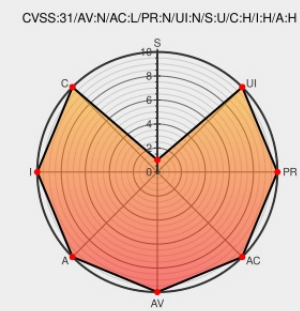
CVE-2020-8599

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

Last Modified on: 07/12/2022 05:42:00 PM UTC

CVE-2020-8599

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Apex One from Trendmicro contain the following vulnerability:

Trend Micro Apex One (2019) and OfficeScan XG server contain a vulnerable EXE file that could allow a remote attacker to write arbitrary data to an arbitrary path on affected installations and bypass ROOT login. Authentication is not required to exploit this vulnerability.

CVE-2020-8599 has been assigned by security@trendmicro.com to track the vulnerability - currently rated as CRITICAL 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: 9.8 - CRITICAL

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

CVSS2 Score: 10 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

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

	success.trendmicro.com text/html	
SECURITY BULLETIN: Multiple Critical Vulnerabilities in Trend Micro Apex One and OfficeScan	Patch Vendor Advisory success.trendmicro.com text/html	MISC success.trendmicro.com/solution/000245571

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

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

cpe:2.3:a:trendmicro:apex_one:2019:*:*:*:*:*:*:*:

cpe:2.3:a:trendmicro:apex_one:2019:*:*:*:*:*:*:*:

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

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

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

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report