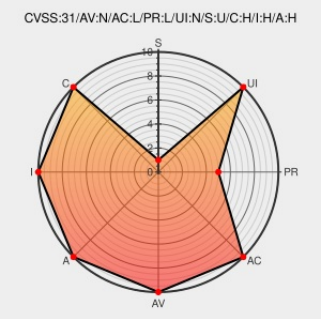
CVE-2020-8468

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

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

CVE-2020-8468

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



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

Trend Micro Apex One (2019), OfficeScan XG and Worry-Free Business Security (9.0, 9.5, 10.0) agents are affected by a content validation escape vulnerability which could allow an attacker to manipulate certain agent client components. An attempted attack requires user authentication.

CVE-2020-8468 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, Trend Micro Worry-Free Business Security (WFBS)** version **OfficeScan XG (12.0), Apex One 2019 (14.0), WFBS 9.0, 9.5 and 10.0**

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 success.trendmicro.com text/html	MISC success.trendmicro.com/jp/solution/000244253
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
SECURITY BULLETIN: Multiple Critical Vulnerabilities in Trend Micro Worry-Free Business Security	Patch Vendor Advisory success.trendmicro.com text/html	MISC success.trendmicro.com/solution/000245572
Q&A | Trend Micro Business Support	Patch Vendor Advisory success.trendmicro.com text/html	MISC success.trendmicro.com/jp/solution/000244836

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
Application	Trendmicro	Worry-free Business Security	10.0	-	All	All
Application	Trendmicro	Worry-free Business Security	10.0	sp1	All	All
Application	Trendmicro	Worry-free Business Security	9.0	sp3	All	All
Application	Trendmicro	Worry-free Business Security	9.5	All	All	All
Application	Trendmicro	Worry-free Business Security	10.0	-	All	All
Application	Trendmicro	Worry-free Business Security	10.0	sp1	All	All
Application	Trendmicro	Worry-free Business Security	9.0	sp3	All	All
Application	Trendmicro	Worry-free Business Security	9.5	All	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:*:*:*:*:*:*:

cpe:2.3:a:trendmicro:worry-free_business_security:10.0:-:*:*:*:*:*:*:

cpe:2.3:a:trendmicro:worry-free_business_security:10.0:sp1:*:*:*:*:*:*:

cpe:2.3:a:trendmicro:worry-free_business_security:9.0:sp3:*:*:*:*:*:*:

cpe:2.3:a:trendmicro:worry-free_business_security:9.5:*:*:*:*:*:*:*:

cpe:2.3:a:trendmicro:worry-free_business_security:10.0:-:*:*:*:*:*:*:

cpe:2.3:a:trendmicro:worry-free_business_security:10.0:sp1:*:*:*:*:*:*:

cpe:2.3:a:trendmicro:worry-free_business_security:9.0:sp3:*:*:*:*:*:*:

cpe:2.3:a:trendmicro:worry-free_business_security:9.5:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@foxbook	「深刻度の高い複数の脆弱性（CVE-2020-8468、CVE-2020-8470、CVE-2020-8598、CVE-2020-8600）が存在する。CVE-2020-8468については、その脆弱性を悪用した実際の攻撃事例が確認… twitter.com/i/web/status/1…	2021-11-29 19:45:53

← Previous ID

Next ID→

© CVE.report 2023 |
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 registred 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.

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