



CVE-2019-18187

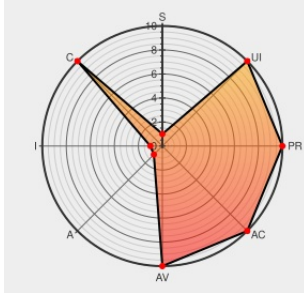
Published on: 10/28/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:06 PM UTC

CVE-2019-18187

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

CVSS:31/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N



Certain versions of [Windows](#) from [Microsoft](#) contain the following vulnerability:

Trend Micro OfficeScan versions 11.0 and XG (12.0) could be exploited by an attacker utilizing a directory traversal vulnerability to extract files from an arbitrary zip file to a specific folder on the OfficeScan server, which could potentially lead to remote code execution (RCE). The remote process execution is bound to a web service account, which depending on the web platform used may have restricted permissions. An attempted attack requires user authentication.

CVE-2019-18187 has been assigned by security@trendmicro.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: **Trend Micro - Trend Micro OfficeScan version Version 11.0, XG (12.0)**

CVSS3 Score: **7.5 - HIGH**

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

CVSS2 Score: **5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
SECURITY BULLETIN: Trend Micro OfficeScan Arbitrary File Upload with Directory Traversal Vulnerability	Vendor Advisory success.trendmicro.com text/html	 MISC success.trendmicro.com/solution/000151730

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
Operating System	Microsoft	Windows	-	All	All	All
Operating System	Microsoft	Windows	-	All	All	All
Application	Trendmicro	Officescan	11.0	sp1	All	All
Application	Trendmicro	Officescan	xg	All	All	All
Application	Trendmicro	Officescan	xg	sp1	All	All
Application	Trendmicro	Officescan	11.0	sp1	All	All
Application	Trendmicro	Officescan	xg	All	All	All
Application	Trendmicro	Officescan	xg	sp1	All	All
cpe:2.3:o:microsoft:windows:-:*:*:*:*:*:						
cpe:2.3:o:microsoft:windows:-:*:*:*:*:*:						
cpe:2.3:a:trendmicro:officescan:11.0:sp1:*:*:*:*:*:						
cpe:2.3:a:trendmicro:officescan:xg:*:*:*:*:*:						
cpe:2.3:a:trendmicro:officescan:xg:sp1:*:*:*:*:*:						
cpe:2.3:a:trendmicro:officescan:11.0: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→

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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)