



CVE-2018-10506

Published on: 06/08/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:21 PM UTC

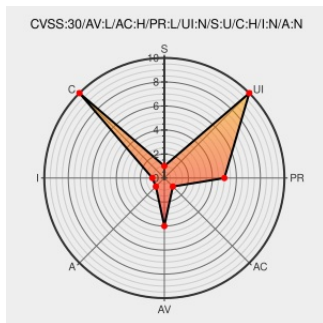
CVE-2018-10506

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



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

A out-of-bounds read information disclosure vulnerability in Trend Micro OfficeScan 11.0 SP1 and XG could allow a local attacker to disclose sensitive information on vulnerable installations due to a flaw within the processing of IOCTL 0x220004 by the TMWFP driver. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.

CVE-2018-10506 has been assigned by security@trendmicro.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **Trend Micro - Trend Micro OfficeScan version 11.0 SP1, XG**

CVSS3 Score: **4.7 - MEDIUM**

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

CVSS2 Score: **1.9 - LOW**

Access Vector	Access Complexity	Authentication
LOCAL	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
-------------	------	------

 CONFIRM success.trendmicro.com/solution/1119961

There are currently no QIDs associated with this CVE

Type	Vendor	Product	Version	Update	Edition	Language
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:a:trendmicro:officescan:xg:sp1:*:*:*:*:*:
```

Next ID→

[site](#). This site includes MITRE data granted under the following [license](#).

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