



CVE-2018-10357

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2018-10357
State	PUBLIC
Assigner	security@trendmicro.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-05-23 16:29:00 UTC
Updated	2018-06-26 18:35:00 UTC
Description	A directory traversal vulnerability in Trend Micro Endpoint Application Control 2.0 could allow a remote attacker to execute c

Risk And Classification

Problem Types: CWE-22

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Trendmicro	Endpoint Application Control	2.0	All	All	All
Application	Trendmicro	Endpoint Application Control	2.0	All	All	All

References

Reference	Source	Link
ZDI-18-469 Zero Day Initiative	MISC	www.zerod
Trend Micro Endpoint Application Control CVE-2018-10357 Directory Traversal Vulnerability	BID	www.secu
Information on the FileDrop Directory Traversal Remote Code Execution Vulnerability - Endpoint Application Control	CONFIRM	success.tr
CVE Program record	CVE.ORG	www.cve.c
NVD vulnerability detail	NVD	nvd.nist.g

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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](#).

Free CVE JSON API [cve.report/api](#)

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