



CVE-2016-6270

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2016-6270
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-01-30 22:59:00 UTC
Updated	2021-09-13 12:04:00 UTC
Description	The handle_certificate function in /vmi/manager/engine/management/commands/apns_worker.py in Trend Micro Virtual Mo

Risk And Classification

Problem Types: CWE-77

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Trendmicro	Virtual Mobile Infrastructure	5.0	All	All	All
Application	Trend Micro	Virtual Mobile Infrastructure	5.0	All	All	All
Application	Trend Micro	Virtual Mobile Infrastructure	5.0	All	All	All

References

Reference	Source	Link	Tag
Remote Code Execution Vulnerability - Virtual Mobile Infrastructure	CONFIRM	success.trendmicro.com	Ver
Trend Micro Bug Hunting - Part III	MISC	qkaiser.github.io	Exp
Trend Micro Virtual Mobile Infrastructure CVE-2016-6270 Remote Code Execution Vulnerability	BID	www.securityfocus.com	Thir
CVE Program record	CVE.ORG	www.cve.org	can
NVD vulnerability detail	NVD	nvd.nist.gov	can

No vendor comments have been submitted for this CVE.

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

© [CVE.report](#) 2026 |

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](#)