



CVE-2018-6671

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

Summary

CVE	CVE-2018-6671
State	PUBLIC
Assigner	psirt@mcafee.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-06-15 14:29:00 UTC
Updated	2023-11-07 03:00:00 UTC
Description	Application Protection Bypass vulnerability in McAfee ePolicy Orchestrator (ePO) 5.3.0 through 5.3.3 and 5.9.0 through 5.9

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mcafee	Epolicy Orchestrator	All	All	All	All
Application	Mcafee	Epolicy Orchestrator	All	All	All	All

References

Reference

- McAfee Security Bulletin - ePolicy Orchestrator update fixes possible localhost only access bypass and sensitive information leak vulnerability
- McAfee ePO 5.9.1 - Registered Executable Local Access Bypass - Windows webapps Exploit
- McAfee ePolicy Orchestrator Bugs Let Remote Authenticate Users Obtain Potentially Sensitive Information and Bypass Access Controls - Sec
- Malformed Request
- CVE Program record
- NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[376557](#) McAfee ePolicy Orchestrator Access Bypass and Aensitive Information Leak Vulnerabilities (SB10240)

© [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](#).

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

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