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)

Free CVE JSON API cve.report/api

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