



CVE-2018-6670

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

Summary

CVE	CVE-2018-6670
State	PUBLIC
Assigner	psirt@mcafee.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-06-07 18:29:00 UTC
Updated	2023-11-07 03:00:00 UTC
Description	External Entity Attack vulnerability in the ePO extension in McAfee Common UI (CUI) 2.0.2 allows remote authenticated users to bypass authentication and execute arbitrary code on the target system.

Risk And Classification

Problem Types: CWE-611

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mcafee	Common Catalog	All	All	All	All
Application	Mcafee	Common Catalog	All	All	All	All

References

Reference	Source	Link
McAfee Security Bulletin - Common Catalog update fixes an XML External Entity Reference vulnerability (CVE-2018-6670)	CONFIRM	kc...
CVE Program record	CVE.ORG	ww...
NVD vulnerability detail	NVD	nvd...

Vendor Comments And Credit

Discovery Credit

LEGACY: McAfee credits Łukasz Juszczuk from ING Business Shared Services B.V. for reporting this flaw.

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](#)