



CVE-2006-5156

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

Summary

CVE	CVE-2006-5156
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-10-05 04:04:00 UTC
Updated	2026-04-23 00:35:47 UTC
Description	Buffer overflow in McAfee ePolicy Orchestrator before 3.5.0.720 and ProtectionPilot before 1.1.1.126 allows remote attacker

Risk And Classification

Primary CVSS: v2.0 10 from nvd@nist.gov

AV:N/AC:L/Au:N/C:C/I:C/A:C

Problem Types: NVD-CWE-Other | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

AV:N/AC:L/Au:N/C:C/I:C/A:C

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mcafee	Epolicy Orchestrator	3.0	All	All	All

Application	Mcafee	Epolicy Orchestrator	3.0	sp2a	All	All
Application	Mcafee	Epolicy Orchestrator	3.5.0	All	All	All
Application	Mcafee	Protectionpilot	1.1.1	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference

- SecurityTracker.com Archives - McAfee ProtectionPilot Buffer Overflow in Processing HTTP Source Headers Lets Remote Users Execute Arb
- IBM X-Force Exchange
- [Full-disclosure] McAfee EPO Buffer Overflow
- McAfee Security Bulletin - ePolicy Orchestrator (ePO) 3.5 Patch 6 or later / ProtectionPilot (PrP)1.1.1 Patch 3 or later fixes vulnerability allowin
- US-CERT Vulnerability Note VU#842452
- www.osvdb.org/29421
- 404 Not Found
- Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
- download.nai.com/products/patches/protectionpilot/v1.1.1/PRP1113.txt
- McAfee ePolicy Orchestrator / ProtectionPilot Source Header Buffer Overflow - Advisories - Secunia
- download.nai.com/products/patches/ePO/v3.5/EPO3506.txt
- knowledge.mcafee.com/SupportSite/search.do
- McAfee EPolicy Orchestrator and ProtectionPilot HTTP Server Remote Buffer Overflow Vulnerability
- SecurityTracker.com Archives - McAfee ePolicy Orchestrator Buffer Overflow in Processing HTTP Source Headers Lets Remote Users Execu
- CVE Program record
- NVD vulnerability detail

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](#).

Free CVE JSON API cve.report/api

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