CVE-2014-1472

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2014-1472
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-01-16 05:05:26 UTC
Updated	2026-04-29 01:13:23 UTC
Description	Multiple cross-site scripting (XSS) vulnerabilities in the Enterprise Manager in McAfee Vulnerability Manager (MVM) 7.5.5 a

Risk And Classification

Primary CVSS: v2.0 4.3 from nvd@nist.gov

AV:N/AC:M/Au:N/C:N/I:P/A:N

EPSS: 0.004990000 probability, percentile 0.659920000 (date 2026-05-03)

Problem Types: CWE-79 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

None

Integrity

Partial

Availability

None

AV:N/AC:M/Au:N/C:N/I:P/A:N

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language

Application	Mcafee	Vulnerability Manager	7.0.11	All	All	All
Application	Mcafee	Vulnerability Manager	7.5.4	All	All	All
Application	Mcafee	Vulnerability Manager	All	All	All	All

Vendor Declared Affected Products

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

References

Reference
osvdb.org/101940
Security Advisory SA56394 - McAfee Vulnerability Manager Cross-Site Scripting and Cross-Site Request Forgery Vulnerabilities - Secunia
McAfee KnowledgeBase - McAfee Security Bulletin – McAfee Vulnerability Manager hotfixes remediate XSS and CSRF vulnerabilities reporte
IBM X-Force Exchange
McAfee Vulnerability Manager Cross Site Scripting and Cross Site Request Forgery Vulnerabilities
McAfee Vulnerability Manager Input Validation Flaw Permits Cross-Site Scripting and Cross-Site Request Forgery Attacks - SecurityTracker
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.