



CVE-2015-7612

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

Summary

CVE	CVE-2015-7612
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-10-01 20:59:08 UTC
Updated	2026-05-06 22:30:45 UTC
Description	Multiple cross-site request forgery (CSRF) vulnerabilities in the Organizations page in Enterprise Manager in McAfee Vulne

Risk And Classification

Primary CVSS: v2.0 6.8 from nvd@nist.gov

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

Problem Types: CWE-352 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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				
McAfee KnowledgeBase - Intel Security - Security Bulletin: Vulnerability Manager 7.5.9 hotfix remediates CSRF vulnerabilities in the MVM Ent				
McAfee Vulnerability Manager Access Control Flaw in 'Organizations' Page Lets Remote Users Conduct Cross-Site Request Forgery Attacks				
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.				