



CVE-2014-6409

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

Summary

CVE	CVE-2014-6409
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-10-06 23:55:08 UTC
Updated	2026-05-06 22:30:45 UTC
Description	Cross-site request forgery (CSRF) vulnerability in M/Monit 3.3.2 and earlier allows remote attackers to hijack the authentication

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	Mmonit	M/monit	All	All	All	All

Vendor Declared Affected Products				
Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified
References				
Reference	Source		Link	T
Full Disclosure: M/Monit - Account hijacking via CSRF	af854a3a-2127-422b-91ae-364da2661108		seclists.org	E
M/Monit 3.3.2 - CSRF Vulnerability	af854a3a-2127-422b-91ae-364da2661108		www.exploit-db.com	E
IBM X-Force Exchange	af854a3a-2127-422b-91ae-364da2661108		exchange.xforce.ibmcloud.com	
M/Monit 3.2.2 Cross Site Request Forgery ≈ Packet Storm	af854a3a-2127-422b-91ae-364da2661108		packetstormsecurity.com	E
CVE Program record	CVE.ORG		www.cve.org	ca
NVD vulnerability detail	NVD		nvd.nist.gov	ca
No vendor comments have been submitted for this CVE.				
There are currently no legacy QID mappings associated with this CVE.				