CVE-2014-3024

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

Summary

CVE	CVE-2014-3024
State	PUBLISHED
Assigner	ibm
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-08-29 09:55:07 UTC
Updated	2026-05-06 22:30:45 UTC
Description	Cross-site request forgery (CSRF) vulnerability in IBM Maximo Asset Management 7.1 through 7.1.1.12 and 7.5 through 7.5

Risk And Classification

Primary CVSS: v2.0 6 from nvd@nist.gov

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

Problem Types: CWE-352 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

Single

Confidentiality

Partial

Integrity

Partial

Availability

Partial

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ibm	Maximo Asset Management	7.1	All	All	All

Application	Ibm	Maximo Asset Management	7.1.1	All	All	All
Application	Ibm	Maximo Asset Management	7.1.1.1	All	All	All
Application	Ibm	Maximo Asset Management	7.1.1.10	All	All	All
Application	Ibm	Maximo Asset Management	7.1.1.11	All	All	All
Application	Ibm	Maximo Asset Management	7.1.1.12	All	All	All
Application	Ibm	Maximo Asset Management	7.1.1.2	All	All	All
Application	Ibm	Maximo Asset Management	7.1.1.5	All	All	All
Application	Ibm	Maximo Asset Management	7.1.1.6	All	All	All
Application	Ibm	Maximo Asset Management	7.1.1.7	All	All	All
Application	Ibm	Maximo Asset Management	7.1.1.8	All	All	All
Application	Ibm	Maximo Asset Management	7.1.1.9	All	All	All
Application	Ibm	Maximo Asset Management	7.1.2	All	All	All
Application	Ibm	Maximo Asset Management	7.5.0.0	All	All	All
Application	Ibm	Maximo Asset Management	7.5.0.1	All	All	All
Application	Ibm	Maximo Asset Management	7.5.0.2	All	All	All
Application	Ibm	Maximo Asset Management	7.5.0.3	All	All	All
Application	Ibm	Maximo Asset Management	7.5.0.4	All	All	All
Application	Ibm	Maximo Asset Management	7.5.0.5	All	All	All
Application	Ibm	Maximo Asset Management	7.5.0.6	All	All	All
Application	Ibm	Smartcloud Control Desk	7.5.0.0	All	All	All
Application	Ibm	Smartcloud Control Desk	7.5.0.1	All	All	All
Application	Ibm	Smartcloud Control Desk	7.5.0.2	All	All	All
Application	Ibm	Smartcloud Control Desk	7.5.0.3	All	All	All
Application	Ibm	Smartcloud Control Desk	7.5.1.0	All	All	All
Application	Ibm	Smartcloud Control Desk	7.5.1.1	All	All	All
Application	Ibm	Smartcloud Control Desk	7.5.1.2	All	All	All

Vendor Declared Affected Products

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

References

Reference
IBM X-Force Exchange
Security Advisory SA60408 - IBM Multiple Products Cross-Site Request Forgery and Security Bypass Vulnerabilities - Secunia
IBM notice: The page you requested cannot be displayed
Security Bulletin: Cross-site Request Forgery Vulnerability Addressed in Asset and Service Management (CVE-2014-3024)

Security Bulletin: Cross-site Request Forgery Vulnerability Addressed in Asset and Service Management (CVE-2014-3024)
IBM Tivoli Change and Configuration Management Database Input Validation Flaw Permits Cross-Site Request Forgery Attacks - SecurityTrac
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.