



CVE-2010-2654

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

Summary

CVE	CVE-2010-2654
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2010-07-08 12:54:00 UTC
Updated	2010-07-20 05:48:00 UTC
Description	Multiple cross-site scripting (XSS) vulnerabilities on the IBM BladeCenter with Advanced Management Module (AMM) firmw

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	ibm	Advanced Management Module	1.00	All	All	All
Hardware	ibm	Advanced Management Module	1.01	All	All	All
Hardware	ibm	Advanced Management Module	1.20	All	All	All
Hardware	ibm	Advanced Management Module	1.20	f	All	All
Hardware	ibm	Advanced Management Module	1.25	All	All	All
Hardware	ibm	Advanced Management Module	1.25	e	All	All
Hardware	ibm	Advanced Management Module	1.25	i	All	All
Hardware	ibm	Advanced Management Module	1.26	b	All	All
Hardware	ibm	Advanced Management Module	1.26	e	All	All
Hardware	ibm	Advanced Management Module	1.26	h	All	All
Hardware	ibm	Advanced Management Module	1.26	i	All	All
Hardware	ibm	Advanced Management Module	1.26	k	All	All
Hardware	ibm	Advanced Management Module	1.28	g	All	All
Hardware	ibm	Advanced Management Module	1.32	d	All	All
Hardware	ibm	Advanced Management Module	1.34	b	All	All
Hardware	ibm	Advanced Management Module	1.34	e	All	All
Hardware	ibm	Advanced Management Module	1.36	d	All	All

Hardware	lbn	Advanced Management Module	1.36	g	All	All
Hardware	lbn	Advanced Management Module	1.36	h	All	All
Hardware	lbn	Advanced Management Module	1.36	k	All	All
Hardware	lbn	Advanced Management Module	1.42	d	All	All
Hardware	lbn	Advanced Management Module	1.42	f	All	All
Hardware	lbn	Advanced Management Module	1.42	i	All	All
Hardware	lbn	Advanced Management Module	1.42	n	All	All
Hardware	lbn	Advanced Management Module	1.42	o	All	All
Hardware	lbn	Advanced Management Module	1.42	t	All	All
Hardware	lbn	Advanced Management Module	2.46	c	All	All
Hardware	lbn	Advanced Management Module	2.46	j	All	All
Hardware	lbn	Advanced Management Module	2.48	c	All	All
Hardware	lbn	Advanced Management Module	2.48	d	All	All
Hardware	lbn	Advanced Management Module	2.48	g	All	All
Hardware	lbn	Advanced Management Module	2.48	n	All	All
Hardware	lbn	Advanced Management Module	2.50	c	All	All
Hardware	lbn	Advanced Management Module	2.50	g	All	All
Hardware	lbn	Advanced Management Module	2.50	k	All	All
Hardware	lbn	Advanced Management Module	2.50	p	All	All
Hardware	lbn	Advanced Management Module	3.54	d	All	All
Hardware	lbn	Advanced Management Module	1.00	All	All	All
Hardware	lbn	Advanced Management Module	1.01	All	All	All
Hardware	lbn	Advanced Management Module	1.20	All	All	All
Hardware	lbn	Advanced Management Module	1.20	f	All	All
Hardware	lbn	Advanced Management Module	1.25	All	All	All
Hardware	lbn	Advanced Management Module	1.25	e	All	All
Hardware	lbn	Advanced Management Module	1.25	i	All	All
Hardware	lbn	Advanced Management Module	1.26	b	All	All
Hardware	lbn	Advanced Management Module	1.26	e	All	All
Hardware	lbn	Advanced Management Module	1.26	h	All	All
Hardware	lbn	Advanced Management Module	1.26	i	All	All
Hardware	lbn	Advanced Management Module	1.26	k	All	All
Hardware	lbn	Advanced Management Module	1.28	g	All	All
Hardware	lbn	Advanced Management Module	1.32	d	All	All
Hardware	lbn	Advanced Management Module	1.34	b	All	All

Hardware	ibm	Advanced Management Module	1.34	e	All	All
Hardware	ibm	Advanced Management Module	1.36	d	All	All
Hardware	ibm	Advanced Management Module	1.36	g	All	All
Hardware	ibm	Advanced Management Module	1.36	h	All	All
Hardware	ibm	Advanced Management Module	1.36	k	All	All
Hardware	ibm	Advanced Management Module	1.42	d	All	All
Hardware	ibm	Advanced Management Module	1.42	f	All	All
Hardware	ibm	Advanced Management Module	1.42	i	All	All
Hardware	ibm	Advanced Management Module	1.42	n	All	All
Hardware	ibm	Advanced Management Module	1.42	o	All	All
Hardware	ibm	Advanced Management Module	1.42	t	All	All
Hardware	ibm	Advanced Management Module	2.46	c	All	All
Hardware	ibm	Advanced Management Module	2.46	j	All	All
Hardware	ibm	Advanced Management Module	2.48	c	All	All
Hardware	ibm	Advanced Management Module	2.48	d	All	All
Hardware	ibm	Advanced Management Module	2.48	g	All	All
Hardware	ibm	Advanced Management Module	2.48	n	All	All
Hardware	ibm	Advanced Management Module	2.50	c	All	All
Hardware	ibm	Advanced Management Module	2.50	g	All	All
Hardware	ibm	Advanced Management Module	2.50	k	All	All
Hardware	ibm	Advanced Management Module	2.50	p	All	All
Hardware	ibm	Advanced Management Module	3.54	d	All	All
Hardware	ibm	Advanced Management Module	All	l	All	All
Hardware	ibm	Advanced Management Module	All	g	All	All
Hardware	ibm	Bladecenter	All	All	All	All
Hardware	ibm	Bladecenter	All	All	All	All

References

Reference	Source	Link
Malformed Request	BID	www.securityfocus.com/bid/66130
66130	OSVDB	osvdb.org
66126	OSVDB	osvdb.org
66128	OSVDB	osvdb.org
Digital Security Research Group - [DSECRG-09-054] IBM Bladecenter Management - Multiple vulnerabilities	MISC	dsecrg.com
IBM Bladecenter Management - Multiple web application vulnerabilities	EXPLOIT-DB	www.exploit-db.com
66122	OSVDB	osvdb.org

66125	OSVDB	osvdb.org
66129	OSVDB	osvdb.org
66127	OSVDB	osvdb.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](#).

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