Open Source Vulnerability Report

BLACKDUCK

Microsoft Demo Project > 3.4

Phase: DEVELOPMENT | Distribution: EXTERNAL

Vulnerability Status Filter: All Vulnerabilities

0 HIGH	3 MEDIUM	0 LOW

VULNERABLE COMPONENTS SUMMARY

Microsoft ASP.NET MVC 5.0.0	0	1	0
jQuery 1.6.2	0	2	0

VULNERABLE COMPONENTS DETAILS

Microsoft ASP.NET MVC 5.0.0

Apache License 2.0 (permissive)

Vulnerability Name	Severity	Base	Exploitability	Impact	Status	Published
CVE-2014-4075	MEDIUM	4.3	2.9	8.6	NEW	08/28/2015

Cross-site scripting (XSS) vulnerability in System.Web.Mvc.dll in Microsoft ASP.NET Model View Controller (MVC) 2.0 through 5.1 allows remote attackers to inject arbitrary web script or HTML via a crafted web page, aka "MVC XSS Vulnerability."

jQuery 1.6.2

GNU General Public License v2.0 or later (reciprocal)

MIT License (permissive)

Vulnerability Name	Severity	Base	Exploitability	Impact	Status	Published
80056	MEDIUM	4.3	2.9	8.6	DUPLICATE	04/11/2017

jQuery Core contains a flaw that allows a DOM-based cross-site scripting (XSS) attack. This flaw exists because the application does not validate certain tags while being rendered using innerHTML. This may allow a context-dependent user to create a specially crafted request that would execute arbitrary script code in a user's browser within the trust relationship between their browser and the underlying library.

CVE-2011-4969	MEDIUM	4.3	2.9	8.6	NEW	11/28/2016

Cross-site scripting (XSS) vulnerability in jQuery before 1.6.3, when using location.hash to select elements, allows remote attackers to inject arbitrary web script or HTML via a crafted tag.

Generated for **HPE Security**
Fortify on Demand

***NOTE**: This report lists **only** the vulnerable components for this Hub project. To view a complete list of Open Source components identified, go to Microsoft Demo Project 3.4.*