

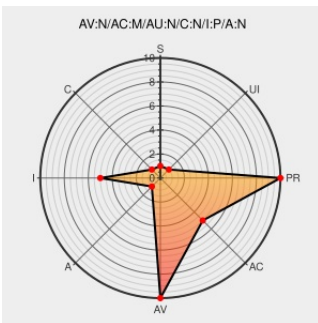


# CVE-2015-6099

Published on: 11/11/2015 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:16 PM UTC

## CVE-2015-6099

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [.net Framework](#) from [Microsoft](#) contain the following vulnerability:

Cross-site scripting (XSS) vulnerability in ASP.NET in Microsoft .NET Framework 4, 4.5, 4.5.1, 4.5.2, and 4.6 allows remote attackers to inject arbitrary web script or HTML via a crafted value, aka ".NET Elevation of Privilege Vulnerability."

CVE-2015-6099 has been assigned by [secure@microsoft.com](mailto:secure@microsoft.com) to track the vulnerability

CVSS2 Score: **4.3 - MEDIUM**

Access  
Vector

**NETWORK**

Access  
Complexity

**MEDIUM**

Authentication

**NONE**

Confidentiality  
Impact

**NONE**

Integrity  
Impact

**PARTIAL**

Availability  
Impact

**NONE**

## CVE References

Description

Tags

Link

Microsoft .NET Framework XSS / Privilege Escalation ≈ Packet Storm

[packetstormsecurity.com](https://packetstormsecurity.com)  
text/html

[MISC  
packetstormsecurity.com/files/134314/Microsoft-.NET-Framework-XSS-Privilege-Escalation.html](https://packetstormsecurity.com/files/134314/Microsoft-.NET-Framework-XSS-Privilege-Escalation.html)

Microsoft Security Bulletin MS15-118 - Important | Microsoft Docs

[docs.microsoft.com](https://docs.microsoft.com)  
text/html

[MS MS15-118](#)

Microsoft .NET Bugs Let Local Users Bypass ASLR and Remote Users Obtain Files and Conduct Cross-Site Scripting Attacks - SecurityTracker

[www.securitytracker.com](https://www.securitytracker.com)  
text/html

[SECTRAK 1034116](#)

SecurityFocus

[www.securityfocus.com](https://www.securityfocus.com)  
text/html

[BUGTRAQ 20151111 Microsoft .NET Framework XSS / Elevation of Privilege CVE-2015-6099](#)

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that

CVESearch is not intended to be used as a source of information for the purpose of determining the severity of a vulnerability, or for any other purpose. CVESearch does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVESearch does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to [comment@cve.report](mailto:comment@cve.report).

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

| Type                                                | Vendor    | Product        | Version | Update | Edition | Language |
|-----------------------------------------------------|-----------|----------------|---------|--------|---------|----------|
| Application                                         | Microsoft | .net Framework | 4.0     | All    | All     | All      |
| Application                                         | Microsoft | .net Framework | 4.5     | All    | All     | All      |
| Application                                         | Microsoft | .net Framework | 4.5.1   | All    | All     | All      |
| Application                                         | Microsoft | .net Framework | 4.5.2   | All    | All     | All      |
| Application                                         | Microsoft | .net Framework | 4.6     | All    | All     | All      |
| Application                                         | Microsoft | .net Framework | 4.0     | All    | All     | All      |
| Application                                         | Microsoft | .net Framework | 4.5     | All    | All     | All      |
| Application                                         | Microsoft | .net Framework | 4.5.1   | All    | All     | All      |
| Application                                         | Microsoft | .net Framework | 4.5.2   | All    | All     | All      |
| Application                                         | Microsoft | .net Framework | 4.6     | All    | All     | All      |
| cpe:2.3:a:microsoft:.net_framework:4.0:*:*:*:*:*:   |           |                |         |        |         |          |
| cpe:2.3:a:microsoft:.net_framework:4.5:*:*:*:*:*:   |           |                |         |        |         |          |
| cpe:2.3:a:microsoft:.net_framework:4.5.1:*:*:*:*:*: |           |                |         |        |         |          |
| cpe:2.3:a:microsoft:.net_framework:4.5.2:*:*:*:*:*: |           |                |         |        |         |          |
| cpe:2.3:a:microsoft:.net_framework:4.6:*:*:*:*:*:   |           |                |         |        |         |          |
| cpe:2.3:a:microsoft:.net_framework:4.0:*:*:*:*:*:   |           |                |         |        |         |          |
| cpe:2.3:a:microsoft:.net_framework:4.5:*:*:*:*:*:   |           |                |         |        |         |          |
| cpe:2.3:a:microsoft:.net_framework:4.5.1:*:*:*:*:*: |           |                |         |        |         |          |
| cpe:2.3:a:microsoft:.net_framework:4.5.2:*:*:*:*:*: |           |                |         |        |         |          |
| cpe:2.3:a:microsoft:.net_framework:4.6:*:*:*:*:*:   |           |                |         |        |         |          |

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

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](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status** [status.cve.report](#)