



CVE-2019-0657

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

Summary

CVE	CVE-2019-0657
State	PUBLIC
Assigner	secure@microsoft.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-03-05 23:29:00 UTC
Updated	2019-03-07 16:55:00 UTC
Description	A vulnerability exists in certain .Net Framework API's and Visual Studio in the way they parse URL's, aka '.NET Framework

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Microsoft	.net Core	1.0	All	All	All
Application	Microsoft	.net Core	2.1	All	All	All
Application	Microsoft	.net Core	2.2	All	All	All
Application	Microsoft	.net Core	1.0	All	All	All
Application	Microsoft	.net Core	2.1	All	All	All
Application	Microsoft	.net Core	2.2	All	All	All
Application	Microsoft	.net Framework	2.0	sp2	All	All
Application	Microsoft	.net Framework	3.0	sp2	All	All
Application	Microsoft	.net Framework	3.5	All	All	All
Application	Microsoft	.net Framework	3.5.1	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	4.6.1	All	All	All
Application	Microsoft	.net Framework	4.6.2	All	All	All
Application	Microsoft	.net Framework	4.7	All	All	All
Application	Microsoft	.net Framework	4.7.1	All	All	All
Application	Microsoft	.net Framework	4.7.2	All	All	All

Application	Microsoft	.net Framework	2.0	sp2	All	All
Application	Microsoft	.net Framework	3.0	sp2	All	All
Application	Microsoft	.net Framework	3.5	All	All	All
Application	Microsoft	.net Framework	3.5.1	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	4.6.1	All	All	All
Application	Microsoft	.net Framework	4.6.2	All	All	All
Application	Microsoft	.net Framework	4.7	All	All	All
Application	Microsoft	.net Framework	4.7.1	All	All	All
Application	Microsoft	.net Framework	4.7.2	All	All	All
Application	Microsoft	Powershell Core	6.0	All	All	All
Application	Microsoft	Powershell Core	6.1	All	All	All
Application	Microsoft	Powershell Core	6.0	All	All	All
Application	Microsoft	Powershell Core	6.1	All	All	All
Application	Microsoft	Visual Studio 2017	-	All	All	All
Application	Microsoft	Visual Studio 2017	15.9	All	All	All
Application	Microsoft	Visual Studio 2017	-	All	All	All
Application	Microsoft	Visual Studio 2017	15.9	All	All	All
Operating System	Microsoft	Windows 10	-	All	All	All
Operating System	Microsoft	Windows 10	1607	All	All	All
Operating System	Microsoft	Windows 10	1703	All	All	All
Operating System	Microsoft	Windows 10	1709	All	All	All
Operating System	Microsoft	Windows 10	1803	All	All	All
Operating System	Microsoft	Windows 10	1809	All	All	All
Operating System	Microsoft	Windows 10	-	All	All	All
Operating System	Microsoft	Windows 10	1607	All	All	All
Operating System	Microsoft	Windows 10	1703	All	All	All
Operating System	Microsoft	Windows 10	1709	All	All	All
Operating System	Microsoft	Windows 10	1803	All	All	All
Operating System	Microsoft	Windows 10	1809	All	All	All
Operating System	Microsoft	Windows 7	-	sp1	All	All
Operating System	Microsoft	Windows 7	-	sp1	All	All
Operating System	Microsoft	Windows 8.1	-	All	All	All
Operating System	Microsoft	Windows 8.1	-	All	All	All

Operating System	Microsoft	Windows Rt 8.1	-	All	All	All
Operating System	Microsoft	Windows Rt 8.1	-	All	All	All
Operating System	Microsoft	Windows Server 2008	-	sp1	All	All
Operating System	Microsoft	Windows Server 2008	-	sp2	All	All
Operating System	Microsoft	Windows Server 2008	r2	sp1	All	All
Operating System	Microsoft	Windows Server 2008	r2	sp1	All	All
Operating System	Microsoft	Windows Server 2008	-	sp1	All	All
Operating System	Microsoft	Windows Server 2008	-	sp2	All	All
Operating System	Microsoft	Windows Server 2008	r2	sp1	All	All
Operating System	Microsoft	Windows Server 2008	r2	sp1	All	All
Operating System	Microsoft	Windows Server 2012	-	All	All	All
Operating System	Microsoft	Windows Server 2012	r2	All	All	All
Operating System	Microsoft	Windows Server 2012	-	All	All	All
Operating System	Microsoft	Windows Server 2012	r2	All	All	All
Operating System	Microsoft	Windows Server 2016	-	All	All	All
Operating System	Microsoft	Windows Server 2016	1709	All	All	All
Operating System	Microsoft	Windows Server 2016	1803	All	All	All
Operating System	Microsoft	Windows Server 2016	-	All	All	All
Operating System	Microsoft	Windows Server 2016	1709	All	All	All
Operating System	Microsoft	Windows Server 2016	1803	All	All	All
Operating System	Microsoft	Windows Server 2019	-	All	All	All
Operating System	Microsoft	Windows Server 2019	-	All	All	All

References

Reference	Source	Link	Tags
Red Hat Customer Portal	REDHAT	access.redhat.com	Third Party A
Microsoft .NET Framework and Visual Studio CVE-2019-0657 Spoofing Vulnerability	BID	www.securityfocus.com	Third Party A
portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0657	CONFIRM	portal.msrc.microsoft.com	Patch, Vendor
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, ar

No vendor comments have been submitted for this CVE.

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

© [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](#) 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](#)