



CVE-2017-8759

Published on: 09/12/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:42 PM UTC

CVE-2017-8759

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

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

Microsoft .NET Framework 2.0, 3.5, 3.5.1, 4.5.2, 4.6, 4.6.1, 4.6.2 and 4.7 allow an attacker to execute code remotely via a malicious document or application, aka ".NET Framework Remote Code Execution Vulnerability."

CVE-2017-8759 has been assigned by [secure@microsoft.com](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: **Microsoft Corporation - Microsoft .NET Framework** version **Microsoft .NET Framework 2.0, 3.5, 3.5.1, 4.5.2, 4.6, 4.6.1, 4.6.2 and 4.7**

CVSS3 Score: **7.8 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **9.3 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Microsoft Windows .NET Framework - Remote Code Execution	Third Party Advisory VDB Entry	EXPLOIT-DB 42711

0000 Execution	VDB Entry www.exploit-db.com Proof of Concept text/html	
Microsoft Windows .NET Framework CVE-2017-8759 Remote Code Execution Vulnerability	Third Party Advisory VDB Entry cve.report (archive) text/html	BID 100742
GitHub - GitHubAssessments/CVE_Assessments_01_2020	github.com text/html	MISC github.com/GitHubAssessments/CVE_Assessments_01_2020
No Description Provided	Patch Vendor Advisory portal.msrc.microsoft.com text/html	CONFIRM portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8759
GitHub - bhdresh/CVE-2017-8759: Exploit toolkit CVE-2017-8759 - v1.0 is a handy python script which provides pentesters and security researchers a quick and effective way to test Microsoft .NET Framework RCE. It could generate a malicious RTF file and deliver metasploit / meterpreter / other payload to victim without any complex configuration.	github.com text/html	MISC github.com/bhdresh/CVE-2017-8759
Microsoft .NET File Processing Flaw Lets Remote Users Execute Arbitrary Code - SecurityTracker	Third Party Advisory VDB Entry www.securitytracker.com text/html	SECTRAK 1039324
GitHub - nccgroup/CVE-2017-8759: NCC Group's analysis and exploitation of CVE-2017-8759 along with further refinements	github.com text/html	MISC github.com/nccgroup/CVE-2017-8759

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 are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Exploit/POC from Github

CVE-2017-8759 微软word漏洞利用脚本

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Microsoft	.net Framework	2.0	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	2.0	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

cpe:2.3:a:microsoft:.net_framework:2.0:sp2:*****:
cpe:2.3:a:microsoft:.net_framework:3.5:*****:
cpe:2.3:a:microsoft:.net_framework:3.5.1:*****:
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:4.6.1:*****:
cpe:2.3:a:microsoft:.net_framework:4.6.2:*****:
cpe:2.3:a:microsoft:.net_framework:4.7:*****:
cpe:2.3:a:microsoft:.net_framework:2.0:sp2:*****:
cpe:2.3:a:microsoft:.net_framework:3.5:*****:
cpe:2.3:a:microsoft:.net_framework:3.5.1:*****:
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:4.6.1:*****:
cpe:2.3:a:microsoft:.net_framework:4.6.2:*****:
cpe:2.3:a:microsoft:.net_framework:4.7:*****:

No vendor comments have been submitted for this CVE

Social Mentions		
Source	Title	Posted (UTC)
	beta shodan in/search?query=v	2021-05-10

 @twittersupport	data.mongodb/search?query=vul...	2021-03-10 16:54:03
 /r/blackhatrussia	Trillium Security MultiSploit Tool v6.5.21 Full	2021-02-23 17:49:37
 /r/tanium	Top 10 Routinely Exploited Vulnerabilities (AA20-133A)	2020-05-27 20:02:50

[← Previous ID](#)
[Next ID →](#)

© CVE.report 2023   |

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](#)