



CVE-2019-0609

Published on: 04/08/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:03 PM UTC

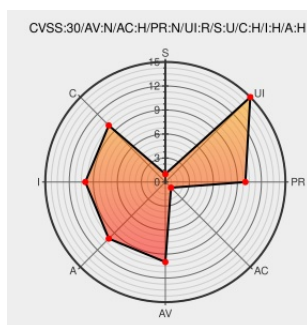
CVE-2019-0609

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Chakracore](#) from [Microsoft](#) contain the following vulnerability:

A remote code execution vulnerability exists in the way the scripting engine handles objects in memory in Microsoft browsers, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0639, CVE-2019-0680, CVE-2019-0769, CVE-2019-0770, CVE-2019-0771, CVE-2019-0773, CVE-2019-0783.

CVE-2019-0609 has been assigned by [secure@microsoft.com](#) to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.5 - HIGH**

Attack Vector

Attack Complexity

Privileges Required

User Interaction

NETWORK

HIGH

NONE

REQUIRED

Scope

Confidentiality Impact

Integrity Impact

Availability Impact

UNCHANGED

HIGH

HIGH

HIGH

CVSS2 Score: **7.6 - HIGH**

Access Vector

Access Complexity

Authentication

NETWORK

HIGH

NONE

Confidentiality Impact

Integrity Impact

Availability Impact

COMPLETE

COMPLETE

COMPLETE

CVE References

Description

Tags

Link

No Description Provided

[Patch](#)

[Vendor Advisory](#)

[portal.msrc.microsoft.com](#)

[CONFIRM portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0609](#)

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.

Related QID Numbers

980956 Dotnet (nuget) Security Update for Microsoft.ChakraCore (GHSA-pjpi-f6r8-56rm)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Microsoft	Chakracore	All	All	All	All
Application	Microsoft	Chakracore	All	All	All	All
Application	Microsoft	Edge	-	All	All	All
Application	Microsoft	Edge	-	All	All	All
Application	Microsoft	Internet Explorer	11	-	All	All
Application	Microsoft	Internet Explorer	11	-	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	r2	sp1	All	All
Operating System	Microsoft	Windows Server 2008	r2	sp1	All	All
Operating System	Microsoft	Windows Server 2016	-	All	All	All
Operating System	Microsoft	Windows Server 2016	-	All	All	All
Operating System	Microsoft	Windows Server 2019	-	All	All	All
Operating System	Microsoft	Windows Server 2019	-	All	All	All
cpe:2.3:a:microsoft:chakracore:*.*.*.*.*.*.*.*.						
cpe:2.3:a:microsoft:chakracore:*.*.*.*.*.*.*.*.						
cpe:2.3:a:microsoft:edge:-:*.*.*.*.*.*.*.*.						
cpe:2.3:a:microsoft:edge:-:*.*.*.*.*.*.*.*.						
cpe:2.3:a:microsoft:internet_explorer:11:-:*.*.*.*.*.*.*.*.						
cpe:2.3:a:microsoft:internet_explorer:11:-:*.*.*.*.*.*.*.*.						
cpe:2.3:o:microsoft:windows_10:-:*.*.*.*.*.*.*.*.						
cpe:2.3:o:microsoft:windows_10:1607:*.*.*.*.*.*.*.*.						
cpe:2.3:o:microsoft:windows_10:1703:*.*.*.*.*.*.*.*.						
cpe:2.3:o:microsoft:windows_10:1709:*.*.*.*.*.*.*.*.						
cpe:2.3:o:microsoft:windows_10:1803:*.*.*.*.*.*.*.*.						
cpe:2.3:o:microsoft:windows_10:1809:*.*.*.*.*.*.*.*.						
cpe:2.3:o:microsoft:windows_10:-:*.*.*.*.*.*.*.*.						
cpe:2.3:o:microsoft:windows_10:1607:*.*.*.*.*.*.*.*.						
cpe:2.3:o:microsoft:windows_10:1703:*.*.*.*.*.*.*.*.						

```
cpe:2.3:o:microsoft:windows_10:1709:*.:.:.:.:.:.:
```

```
cpe:2.3:o:microsoft:windows 10:1803:*.~*~*~*~*~*~*
```

```
cpe:2.3:o:microsoft:windows 10:1809:*.~*~*~*~*~*~*
```

```
cpe:2.3:o:microsoft:windows 7:-sp1:*:*:*:*.*
```

```
cpe:2.3:o:microsoft:windows_7:-:sp1:*:*:*:*:*:
```

```
cpe:2.3:o:microsoft:windows_8.1:-:*:*:*:*:*:*:
```

```
cpe:2.3:o:microsoft:windows 8.1:-:*:*:*:*:*:
```

```
cpe:2.3:o:microsoft:windows rt 8.1:-:*:*:*:*:*:
```

```
cpe:2.3:o:microsoft:windows rt 8.1:-:*:*:*:*:*:
```

```
cpe:2.3:o:microsoft:windows_server_2008:r2:sp1:*:*:*:x64:*
```

```
cpe:2.3:o:microsoft:windows_server_2008:r2:sp1:.*.*.*:x64:.*
```

```
cpe:2.3:o:microsoft:windows_server_2016:-:*:*:*:*:*.*
```

```
cpe:2.3:o:microsoft:windows server 2016:-:*:*:*:*:*:*
```

```
cpe:2.3:o:microsoft:windows server 2019:-:*:*:*:*:*:*
```

```
cpe:2.3:o:microsoft:windows server 2019:-:*:*:*:*:*:*
```

No vendor comments have been submitted for this CVE

[← Previous ID](#)

Next ID→

© CVE.report 2024 |

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