



CVE-2017-8634

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

Summary

CVE	CVE-2017-8634
State	PUBLIC
Assigner	secure@microsoft.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-08-08 21:29:00 UTC
Updated	2019-03-19 19:08:00 UTC
Description	Microsoft Edge in Microsoft Windows 10 1703 allows an attacker to execute arbitrary code in the context of the current user

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Microsoft	Edge	-	All	All	All
Application	Microsoft	Edge	-	All	All	All
Operating System	Microsoft	Windows 10	1703	All	All	All
Operating System	Microsoft	Windows 10	1703	All	All	All

References

Reference
Microsoft Edge Chakra - 'JavascriptArray::ConcatArgs' Type Confusion - Windows dos Exploit
Microsoft Edge CVE-2017-8634 Scripting Engine Remote Memory Corruption Vulnerability
portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8634
Microsoft Edge Object Memory Handling Flaws in Scripting Engines Let Remote Users Execute Arbitrary Code, Bypass a Security Feature, ar
CVE Program record
NVD vulnerability detail

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](#).

Free CVE JSON API [cve.report/api](#)

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