



CVE-2017-0135

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

Summary

CVE	CVE-2017-0135
State	PUBLIC
Assigner	secure@microsoft.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-03-17 00:59:00 UTC
Updated	2019-10-03 00:03:00 UTC
Description	Microsoft Edge allows remote attackers to bypass the Same Origin Policy for HTML elements in other browser windows, ak

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Microsoft	Edge	All	All	All	All
Application	Microsoft	Edge	All	All	All	All

References

Reference
Bypass CSP by Abusing XSS Filter in Edge – InfoSec Writeups – Medium
Microsoft Edge Multiple Flaws Let Remote Users Bypass Security Restrictions, Spoof URLs, Obtain Potentially Sensitive Information, and Exe
CVE-2017-0135漏洞分析：利用Edge浏览器的XSS过滤器绕过CSP - FreeBuf互联网安全新媒体平台 关注黑客与极客
Security Update Guide - Microsoft Security Response Center
Microsoft Edge CVE-2017-0135 Security Bypass Vulnerability
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](#)