



CVE-2016-3295

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

Summary

CVE	CVE-2016-3295
State	PUBLISHED
Assigner	microsoft
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-09-14 10:59:09 UTC
Updated	2026-05-06 22:30:45 UTC
Description	Microsoft Internet Explorer 10 and 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory consumption) via crafted HTML documents, as demonstrated by a denial of service (memory consumption) attack against Microsoft Edge. CVE-2016-3295 is a memory consumption issue in Microsoft Edge. A remote attacker can cause a denial of service (memory consumption) attack against Microsoft Edge by sending a crafted HTML document to the browser. The attacker can cause the browser to consume a large amount of memory, which can lead to a denial of service (memory consumption) attack. CVE-2016-3295 is a memory consumption issue in Microsoft Internet Explorer 10 and 11. A remote attacker can cause a denial of service (memory consumption) attack against Microsoft Internet Explorer 10 and 11 by sending a crafted HTML document to the browser. The attacker can cause the browser to consume a large amount of memory, which can lead to a denial of service (memory consumption) attack.

Risk And Classification

Primary CVSS: v3.0 7.5 HIGH from nvd@nist.gov

CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H

EPSS: 0.213700000 probability, percentile 0.957290000 (date 2026-05-06)

Problem Types: CWE-119 | n/a

Version	Source	Type	Score	Severity	Vector
3.0	nvd@nist.gov	Primary	7.5	HIGH	CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H
2.0	nvd@nist.gov	Primary	5.1		AV:N/AC:H/Au:N/C:P/I:P/A:P

CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

High

Integrity

High

High

Availability

High

CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

High

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

AV:N/AC:H/Au:N/C:P/I:P/A:P

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Microsoft	Edge	-	All	All	All
Application	Microsoft	Internet Explorer	10	All	All	All
Application	Microsoft	Internet Explorer	11	-	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference
Microsoft Edge Multiple Flaws Let Remote Users Obtain Potentially Sensitive Information and Execute Arbitrary Code - SecurityTracker
Microsoft Security Bulletin MS16-104 - Critical Microsoft Docs
Microsoft Internet Explorer Multiple Flaws Let Remote Users Obtain Potentially Sensitive Information, Bypass Security, Execute Arbitrary Code
Microsoft Security Bulletin MS16-105 - Critical Microsoft Docs
www.securityfocus.com/bid/92830
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](#)