



# CVE-2016-7200

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

## Summary

<b>CVE</b>	CVE-2016-7200
<b>State</b>	PUBLISHED
<b>Assigner</b>	microsoft
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2016-11-10 06:59:15 UTC
<b>Updated</b>	2026-04-22 13:51:50 UTC
<b>Description</b>	The Chakra JavaScript scripting engine in Microsoft Edge allows remote attackers to execute arbitrary code or cause a den

## Risk And Classification

**Primary CVSS:** v3.1 8.8 HIGH from nvd@nist.gov

**CVSS:** 3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

**EPSS:** 0.882580000 probability, percentile 0.994980000 (date 2026-04-25)

**CISA KEV:** Listed on 2022-03-28; due 2022-04-18; ransomware use Unknown

**Problem Types:** CWE-787 | n/a | CWE-787 CWE-787 Out-of-bounds Write

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
3.1	ADP	DECLARED	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
2.0	nvd@nist.gov	Primary	7.6		AV:N/AC:H/Au:N/C:C/I:C/A:C

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:N/AC:L/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

Complete

Integrity

Complete

Availability

Complete

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

### CISA Known Exploited Vulnerability

<b>Vendor</b>	Microsoft
<b>Product</b>	Edge
<b>Name</b>	Microsoft Edge Memory Corruption Vulnerability
<b>Required Action</b>	Apply updates per vendor instructions.
<b>Notes</b>	<a href="https://nvd.nist.gov/vuln/detail/CVE-2016-7200">https://nvd.nist.gov/vuln/detail/CVE-2016-7200</a>

### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Microsoft	Edge	-	All	All	All
Operating System	Microsoft	Windows 10 1507	-	All	All	All
Operating System	Microsoft	Windows 10 1511	-	All	All	All
Operating System	Microsoft	Windows 10 1607	-	All	All	All
Operating System	Microsoft	Windows Server 2016	-	-	All	All

### Vendor Declared Affected Products

Vendor Declared Affected Products

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

References

Reference
<a href="http://www.cisa.gov/known-exploited-vulnerabilities-catalog">www.cisa.gov/known-exploited-vulnerabilities-catalog</a>
Microsoft Edge CVE-2016-7200 Scripting Engine Remote Memory Corruption Vulnerability
Microsoft Edge Multiple Flaws Let Remote Users Obtain Potentially Sensitive Information, Access Files, Spoof Content, and Execute Arbitrary
GitHub - teori-io/chakra-2016-11: Proof-of-Concept exploit for Edge bugs (CVE-2016-7200 & CVE-2016-7201)
Microsoft Edge (Windows 10) - 'chakra.dll' Information Leak / Type Confusion Remote Code Execution
Microsoft Edge - 'Array.filter' Information Leak - Windows dos Exploit
Microsoft Edge chakra.dll Information Leak / Type Confusion ≈ Packet Storm
Microsoft Security Bulletin MS16-129 - Critical   Microsoft Docs
CVE Program record
NVD vulnerability detail
CISA Known Exploited Vulnerabilities catalog

No vendor comments have been submitted for this CVE.

Additional Advisory Data

Source	Time	Event
ADP	2022-03-28T00:00:00.000Z	CVE-2016-7200 added to CISA KEV

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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](#).

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

CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)