

CVE-2018-8298

ChakraCore Scripting Engine Type Confusion Vulnerability

CISA KEV since Mar 3, 2022

Actively exploited

A remote code execution vulnerability exists in the way that the ChakraCore scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability." This affects ChakraCore. This CVE ID is unique from CVE-2018-8242, CVE-2018-8283, CVE-2018-8287, CVE-2018-8288, CVE-2018-8291, CVE-2018-8296.

EVRS 77 / ₁₀₀ Urgent priority	CVSS V3.1 7.5 High · NVD	EPSS 0.747 99.5th percentile · FIRST	CISA DEADLINE Mar 17, 2022 KEV since 2022 · listed over a year
---	--	--	--

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.747 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 7.5	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: Apply updates per vendor instructions.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
Microsoft.ChakraCore	< 1.10.1	1.10.1	GitHub
chakracore	< 1.10.1	1.10.1	NVD

Sources

Vendor guidance	portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8298	NVD	nvd.nist.gov/vuln/detail/CVE-2018-8298
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	GitHub advisory	github.com/advisories/GHSA-wgw2-wwq8-c7wf
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2022-5575	Current data	evulnable.com/vulnerability-management/cve/CVE-2018-8298

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.