



CVE-2018-0980

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

Summary

CVE	CVE-2018-0980
State	PUBLIC
Assigner	secure@microsoft.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-04-12 01:29:00 UTC
Updated	2020-08-24 17:37:00 UTC
Description	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Micro

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Microsoft	Chakracore	All	All	All	All
Application	Microsoft	Chakracore	All	All	All	All
Application	Microsoft	Edge	All	All	All	All
Application	Microsoft	Edge	All	All	All	All
Operating System	Microsoft	Windows 10	-	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 10	1703	All	All	All
Operating System	Microsoft	Windows 10	1709	All	All	All
Operating System	Microsoft	Windows 10	-	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 10	1703	All	All	All
Operating System	Microsoft	Windows 10	1709	All	All	All
Operating System	Microsoft	Windows Server 2016	-	All	All	All
Operating System	Microsoft	Windows Server 2016	-	All	All	All

References
Reference
Microsoft ChakraCore Scripting Engine CVE-2018-0980 Remote Memory Corruption Vulnerability
Microsoft Edge Chakra JIT - Bound Check Elimination Bug - Windows dos Exploit
portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0980
Microsoft Edge Multiple Object Memory Handling Errors Let Remote Users Execute Arbitrary Code and Obtain Potentially Sensitive Information
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.