CVE-2018-8551

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2018-8551
State	PUBLIC
Assigner	secure@microsoft.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-11-14 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
Application	Microsoft	Chakracore	-	All	All	All
Application	Microsoft	Edge	-	All	All	All
Application	Microsoft	Edge	-	All	All	All
Operating System	Microsoft	Windows 10	All	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	1803	All	All	All
Operating System	Microsoft	Windows 10	1809	All	All	All
Operating System	Microsoft	Windows 10	All	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	1803	All	All	All
Operating System	Microsoft	Windows 10	1809	All	All	All
Operating System	Microsoft	Windows Server 2019	-	All	All	All

Operating System	Microsoft	Windows Server 2019	-	All	All	All

References

Reference
portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8551
Microsoft ChakraCore Scripting Engine CVE-2018-8551 Remote Memory Corruption Vulnerability
Microsoft Edge Multiple Bugs Let Remote Users Execute Arbitrary Code and Obtain Conduct Cross-Site Scripting Attacks on the Target Syste
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.