CVE-2017-11861

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

Summary

CVE	CVE-2017-11861
State	PUBLIC
Assigner	secure@microsoft.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-11-15 03:29:00 UTC
Updated	2022-05-23 17:29:00 UTC
Description	Microsoft Edge in Windows 10 1607, 1703, 1709, Windows Server 2016 and Windows Server, version 1709 allows an attac

Risk And Classification

Problem Types: CWE-119

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
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	1709	All	All	All
Operating System	Microsoft	Windows Server	1709	All	All	All
Operating System	Microsoft	Windows Server 2016	-	All	All	All

Operating System	Microsoft	Windows Server 2016	-	All	All	All

References

Reference	Source	Link
Microsoft Edge Multiple Object Memory Handling Flaws Lets Remote Users Execute Arbitrary Code - SecurityTracker	SECTRACK	www.
Microsoft Edge Scripting Engine CVE-2017-11861 Remote Memory Corruption Vulnerability	BID	www.
portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11861	CONFIRM	porta
Microsoft Edge Chakra: JIT - 'Lowerer::LowerBoundCheck' Incorrect Integer Overflow Check - Windows dos Exploit	EXPLOIT-DB	www.
CVE Program record	CVE.ORG	www.
NVD vulnerability detail	NVD	nvd.n

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**