



CVE-2019-0696

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

Summary

CVE	CVE-2019-0696
State	PUBLIC
Assigner	secure@microsoft.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-04-09 00:29:00 UTC
Updated	2020-08-24 17:37:00 UTC
Description	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Wind

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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	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 2016	-	All	All	All
Operating System	Microsoft	Windows Server 2016	1709	All	All	All
Operating System	Microsoft	Windows Server 2016	1803	All	All	All
Operating System	Microsoft	Windows Server 2016	-	All	All	All
Operating System	Microsoft	Windows Server 2016	1709	All	All	All
Operating System	Microsoft	Windows Server 2016	1803	All	All	All
Operating System	Microsoft	Windows Server 2019	-	All	All	All

Operating System	Microsoft	Windows Server 2019	-	All	All	All
References						
Reference	Source		Link	Tags		
portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0696	CONFIRM		portal.msrc.microsoft.com	Patch, Vendor Advis		
CVE Program record	CVE.ORG		www.cve.org	canonical		
NVD vulnerability detail	NVD		nvd.nist.gov	canonical, analysis		
No vendor comments have been submitted for this CVE.						
There are currently no legacy QID mappings associated with this CVE.						