CVE-2018-8449

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

Summary

CVE	CVE-2018-8449
State	PUBLIC
Assigner	secure@microsoft.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-09-13 00:29:00 UTC
Updated	2019-10-03 00:03:00 UTC
Description	A security feature bypass exists when Device Guard incorrectly validates an untrusted file, aka "Device Guard Security Fea

Risk And Classification

Problem Types: CWE-367

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Microsoft	Windows 10	-	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	-	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 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

References

Reference	Source
portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8449	CONFIRM
Microsoft Windows Device Guard CVE-2018-8449 Remote Security Bypass Vulnerability	BID
Microsoft Windows - 'CiSetFileCache' WDAC Security Feature Bypass TOCTOU - Windows dos Exploit	EXPLOIT-DB
Microsoft Windows Device Guard Lets Local Users Bypass Trusted File Restrictions on the Target System - SecurityTracker	SECTRACK
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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