



CVE-2018-8406

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

Summary

CVE	CVE-2018-8406
State	PUBLIC
Assigner	secure@microsoft.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-08-15 17:29:00 UTC
Updated	2019-10-03 00:03:00 UTC
Description	An elevation of privilege vulnerability exists when the DirectX Graphics Kernel (DXGKRNL) driver improperly handles objec

Risk And Classification

EPSS: 0.499900000 probability, percentile 0.978500000 (date 2026-05-16)

CISA KEV: Listed on 2022-03-28; due 2022-04-18; ransomware use Known

Problem Types: CWE-404

CISA Known Exploited Vulnerability

Vendor	Microsoft
Product	DirectX Graphics Kernel (DXGKRNL)
Name	Microsoft DirectX Graphics Kernel Privilege Escalation Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://nvd.nist.gov/vuln/detail/CVE-2018-8406

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	Link
Microsoft DirectX Graphics Kernel Driver Bugs Let Local Users Gain Elevated Privileges - SecurityTracker	SECTRACK	www.securitytrack.com
Microsoft Windows DirectX Graphics Kernel CVE-2018-8406 Local Privilege Escalation Vulnerability	BID	www.securityfocus.com
portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8406	CONFIRM	portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8406
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov
CISA Known Exploited Vulnerabilities catalog	CISA	www.cisa.gov

No vendor comments have been submitted for this CVE.

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

© CVE.report 2026 |
 Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](http://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](http://www.mitre.org). This site includes MITRE data granted under the following [license](http://www.mitre.org).

Free CVE JSON API cve.report/api

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