CVE-2020-16968

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-16968
State	PUBLIC
Assigner	secure@microsoft.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-10-16 23:15:00 UTC
Updated	2023-12-31 20:15:00 UTC
Description	A remote code execution vulnerability exists when the Windows Camera Codec Pack improperly handles objects in memory

Risk And Classification

Problem Types: CWE-20 | CWE-787

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	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	1903	All	All	All
Operating System	Microsoft	Windows 10	1909	All	All	All
Operating System	Microsoft	Windows 10	2004	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	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	1903	All	All	All
Operating System	Microsoft	Windows 10	1909	All	All	All
Operating System	Microsoft	Windows 10	2004	All	All	All

References

Reference	Source	Link	Tags
portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16968	MISC	portal.msrc.microsoft.com	Patch, Vendor Adv
ZDI-20-1258 | Zero Day Initiative	MISC	www.zerodayinitiative.com	Third Party Adviso
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.