



Microsoft Streaming Service Proxy Privilege Escalation Vulnerability

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

Summary

CVE	CVE-2023-36802
State	PUBLIC
Assigner	secure@microsoft.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-09-12 17:15:00 UTC
Updated	2023-09-14 20:09:00 UTC
Description	Microsoft Streaming Service Proxy Elevation of Privilege Vulnerability

Risk And Classification

EPSS: 0.754340000 probability, percentile 0.989060000 (date 2026-05-04)

CISA KEY: Listed on 2023-09-12; due 2023-10-03; ransomware use Unknown

Problem Types: NVD-CWE-noinfo

CISA Known Exploited Vulnerability

Vendor	Microsoft
Product	Streaming Service Proxy
Name	Microsoft Streaming Service Proxy Privilege Escalation Vulnerability
Required Action	Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.
Notes	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36802 ; https://nvd.nist.gov/vuln/detail/CVE-2023-36802

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Microsoft	Windows 10 1809	All	All	All	All
Operating System	Microsoft	Windows 10 21h2	All	All	All	All
Operating System	Microsoft	Windows 10 22h2	All	All	All	All
Operating System	Microsoft	Windows 11 21h2	All	All	All	All
Operating System	Microsoft	Windows 11 22h2	All	All	All	All
Operating System	Microsoft	Windows Server 2019	-	All	All	All
Operating System	Microsoft	Windows Server 2022	-	All	All	All

Operating System	MICROSOFT	WINDOWS SERVER 2022	-	All	All	All
References						
Reference	Source	Link	Tags			
Security Update Guide - Microsoft Security Response Center	MISC	msrc.microsoft.com				
CVE Program record	CVE.ORG	www.cve.org	canonical			
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis			
CISA Known Exploited Vulnerabilities catalog	CISA	www.cisa.gov	kev			
No vendor comments have been submitted for this CVE.						
There are currently no legacy QID mappings associated with this CVE.						

© [CVE.report](https://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](https://mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://mitre.org/cve). This site includes MITRE data granted under the following [license](https://mitre.org/cve).

Free CVE JSON API cve.report/api

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