



CVE-2023-36799

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

Summary

CVE	CVE-2023-36799
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 20:21:00 UTC
Description	.NET Core and Visual Studio Denial of Service Vulnerability

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Microsoft	.net	6.0.0	-	All	All
Application	Microsoft	.net	7.0.0	All	All	All
Application	Microsoft	Visual Studio 2022	All	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

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[160908](#) Oracle Enterprise Linux Security Update for .net 7.0 (ELSA-2023-5145)

[160909](#) Oracle Enterprise Linux Security Update for .net 7.0 (ELSA-2023-5146)

[160910](#) Oracle Enterprise Linux Security Update for .net 6.0 (ELSA-2023-5144)

[160911](#) Oracle Enterprise Linux Security Update for .net 6.0 (ELSA-2023-5143)

161039 Oracle Enterprise Linux Security Update for .net 7.0 (ELSA-2023-6247)
161041 Oracle Enterprise Linux Security Update for .net 6.0 (ELSA-2023-6242)
161042 Oracle Enterprise Linux Security Update for .net 7.0 (ELSA-2023-6246)
161047 Oracle Enterprise Linux Security Update for .net 6.0 (ELSA-2023-6245)
199905 Ubuntu Security Notification for .NET Vulnerabilities (USN-6438-1)
199921 Ubuntu Security Notification for .Net regressions Vulnerability (USN-6438-2)
242264 Red Hat Update for .net 7.0 (RHSA-2023:6247)
242265 Red Hat Update for .net 6.0 (RHSA-2023:6245)
242266 Red Hat Update for .net 6.0 security (RHSA-2023:6249)
242267 Red Hat Update for .net 7.0 (RHSA-2023:6246)
242268 Red Hat Update for .net 6.0 (RHSA-2023:6242)
356385 Amazon Linux Security Advisory for dotnet6.0 : ALAS2023-2023-369
503316 Alpine Linux Security Update for dotnet7-build
503317 Alpine Linux Security Update for dotnet7-runtime
503440 Alpine Linux Security Update for dotnet6-build
503441 Alpine Linux Security Update for dotnet6-runtime
503442 Alpine Linux Security Update for dotnet7-build
503444 Alpine Linux Security Update for dotnet7-runtime
506006 Alpine Linux Security Update for dotnet6-build
506008 Alpine Linux Security Update for dotnet6-build
506014 Alpine Linux Security Update for dotnet6-runtime
506016 Alpine Linux Security Update for dotnet6-runtime
506022 Alpine Linux Security Update for dotnet7-build
506024 Alpine Linux Security Update for dotnet7-build
506027 Alpine Linux Security Update for dotnet7-runtime
506029 Alpine Linux Security Update for dotnet7-runtime
92119 Microsoft Visual Studio Multiple Vulnerabilities
941251 AlmaLinux Security Update for .NET (ALSA-2023:5146)

941252 AlmaLinux Security Update for .NET (ALSA-2023:5143)
941255 AlmaLinux Security Update for .NET (ALSA-2023:5144)
941256 AlmaLinux Security Update for .NET (ALSA-2023:5145)
941336 AlmaLinux Security Update for .NET (ALSA-2023:6246)
941337 AlmaLinux Security Update for .NET (ALSA-2023:6242)
941339 AlmaLinux Security Update for .NET (ALSA-2023:6245)
941340 AlmaLinux Security Update for .NET (ALSA-2023:6247)
961017 Rocky Linux Security Update for .NET (RLSA-2023:5144)
961067 Rocky Linux Security Update for .NET (RLSA-2023:6242)
961073 Rocky Linux Security Update for .NET (RLSA-2023:6245)

© [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](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)