



Microsoft .NET Core and Visual Studio Denial-of-Service Vulnerability

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

Summary

CVE	CVE-2023-38180
State	PUBLIC
Assigner	secure@microsoft.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-08-08 19:15:00 UTC
Updated	2023-08-20 03:15:00 UTC
Description	.NET and Visual Studio Denial of Service Vulnerability

Risk And Classification

EPSS: 0.008820000 probability, percentile 0.754360000 (date 2026-04-22)

CISA KEV: Listed on 2023-08-09; due 2023-08-30; ransomware use Unknown

Problem Types: NVD-CWE-noinfo

CISA Known Exploited Vulnerability

Vendor	Microsoft
Product	.NET Core and Visual Studio
Name	Microsoft .NET Core and Visual Studio Denial-of-Service 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/en-US/vulnerability/CVE-2023-38180 ; https://nvd.nist.gov/vuln/detail/CVE-2023-38180

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	Asp.net Core	2.1	All	All	All
Application	Microsoft	Visual Studio 2022	All	All	All	All

References

Reference	Source	Link
-----------	--------	------

[SECURITY] Fedora 37 Update: dotnet7.0-7.0.110-1.fc37 - package-announce - Fedora Mailing-Lists	MISC	lists.fedoraproject.org
Security Update Guide - Microsoft Security Response Center	MISC	msrc.microsoft.com
[SECURITY] Fedora 38 Update: dotnet7.0-7.0.110-1.fc38 - package-announce - Fedora Mailing-Lists	MISC	lists.fedoraproject.org
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.

Legacy QID Mappings

[160871](#) Oracle Enterprise Linux Security Update for .net 6.0 (ELSA-2023-4645)

[160872](#) Oracle Enterprise Linux Security Update for .net 6.0 (ELSA-2023-4644)

[160873](#) Oracle Enterprise Linux Security Update for .net 7.0 (ELSA-2023-4642)

[160874](#) Oracle Enterprise Linux Security Update for .net 7.0 (ELSA-2023-4643)

[199643](#) Ubuntu Security Notification for .NET Vulnerabilities (USN-6278-1)

[199647](#) Ubuntu Security Notification for .NET Vulnerabilities (USN-6278-2)

[241945](#) Red Hat Update for .net 6.0 (RHSA-2023:4639)

[241947](#) Red Hat Update for .net 6.0 (RHSA-2023:4640)

[241948](#) Red Hat Update for .net 7.0 security (RHSA-2023:4643)

[241949](#) Red Hat Update for .net 6.0 security (RHSA-2023:4645)

[241950](#) Red Hat Update for rh-dotnet60-dotnet security (RHSA-2023:4641)

[241952](#) Red Hat Update for .net 6.0 security (RHSA-2023:4644)

[241953](#) Red Hat Update for .net 7.0 security (RHSA-2023:4642)

[284428](#) Fedora Security Update for dotnet6.0 (FEDORA-2023-cbc688b8ca)

[284429](#) Fedora Security Update for dotnet6.0 (FEDORA-2023-25112489ab)

[503161](#) Alpine Linux Security Update for dotnet6-build

[503165](#) Alpine Linux Security Update for dotnet6-runtime

[503169](#) Alpine Linux Security Update for dotnet7-build

[503170](#) Alpine Linux Security Update for dotnet7-runtime

[506005](#) Alpine Linux Security Update for dotnet6-build

506013 Alpine Linux Security Update for dotnet6-runtime
506021 Alpine Linux Security Update for dotnet7-build
506026 Alpine Linux Security Update for dotnet7-runtime
92047 Microsoft .NET Security Update for August 2023
92052 Microsoft Visual Studio Security Updates for August 2023
941230 AlmaLinux Security Update for .NET (ALSA-2023:4644)
941231 AlmaLinux Security Update for .NET (ALSA-2023:4642)
941233 AlmaLinux Security Update for .NET (ALSA-2023:4643)
941234 AlmaLinux Security Update for .NET (ALSA-2023:4645)
941420 AlmaLinux Security Update for .NET (ALSA-2023:4645)
961031 Rocky Linux Security Update for .NET (RLSA-2023:4645)
961038 Rocky Linux Security Update for .NET (RLSA-2023:4643)
994793 DotNet (Nugget) Security Update for Microsoft.AspNetCore.App.Runtime.win-arm64 (GHSA-vmch-3w2x-vhgg)

© [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](#).

Free CVE JSON API [cve.report/api](#)

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