



# CVE-2023-33170

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

|                        |   |
|------------------------|---|
| <b>CVE</b>             | CVE-2023-33170  |
| <b>State</b>           | PUBLIC  |
| <b>Assigner</b>        | secure@microsoft.com  |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                    |
| <b>Published</b>       | 2023-07-11 18:15:00 UTC   |
| <b>Updated</b>         | 2023-07-31 17:47:00 UTC   |
| <b>Description</b>     | ASP.NET and Visual Studio Security Feature Bypass Vulnerability |

## Risk And Classification

**Problem Types:** CWE-362

## NVD Known Affected Configurations (CPE 2.3)

| Type             | Vendor                        | Product                            | Version | Update | Edition | Language |
|------------------|-------------------------------|------------------------------------|---------|--------|---------|----------|
| Operating System | <a href="#">Fedoraproject</a> | <a href="#">Fedora</a>             | 37      | All    | All     | All      |
| Operating System | <a href="#">Fedoraproject</a> | <a href="#">Fedora</a>             | 38      | All    | All     | All      |
| Application      | <a href="#">Microsoft</a>     | <a href="#">.net</a>               | All     | All    | All     | All      |
| Application      | <a href="#">Microsoft</a>     | <a href="#">Visual Studio 2022</a> | All     | All    | All     | All      |

## References

| Reference   | Source  | Link  |
|---|---------|---|
| Security Update Guide - Microsoft Security Response Center                                      | MISC    | <a href="https://msrc.microsoft.com">msrc.microsoft.com</a>           |
| [SECURITY] Fedora 38 Update: dotnet7.0-7.0.109-1.fc38 - package-announce - Fedora Mailing-Lists | MISC    | <a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a> |
| [SECURITY] Fedora 37 Update: dotnet6.0-6.0.120-1.fc37 - package-announce - Fedora Mailing-Lists | MISC    | <a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a> |
| [SECURITY] Fedora 38 Update: dotnet6.0-6.0.120-1.fc38 - package-announce - Fedora Mailing-Lists | MISC    | <a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a> |
| [SECURITY] Fedora 37 Update: dotnet7.0-7.0.109-1.fc37 - package-announce - Fedora Mailing-Lists | MISC    | <a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a> |
| CVE Program record  | CVE.ORG | <a href="https://www.cve.org">www.cve.org</a>                         |
| NVD vulnerability detail  | NVD     | <a href="https://nvd.nist.gov">nvd.nist.gov</a>                       |

No vendor comments have been submitted for this CVE.

## Legacy OID Mappings

|  |
|--|
| 160784 Oracle Enterprise Linux Security Update for .net 6.0 (ELSA-2023-4059) |
| 160785 Oracle Enterprise Linux Security Update for .net 6.0 (ELSA-2023-4060) |
| 160795 Oracle Enterprise Linux Security Update for .net 7.0 (ELSA-2023-4057) |
| 160796 Oracle Enterprise Linux Security Update for .net 7.0 (ELSA-2023-4058) |
| 199459 Ubuntu Security Notification for .NET Vulnerability (USN-6217-1)      |
| 241797 Red Hat Update for .net 7.0 security (RHSA-2023:4057)                 |
| 241798 Red Hat Update for .net 6.0 security (RHSA-2023:4061)                 |
| 241799 Red Hat Update for .net 7.0 security (RHSA-2023:4058)                 |
| 241805 Red Hat Update for .net 6.0 security (RHSA-2023:4059)                 |
| 241811 Red Hat Update for .net 6.0 security (RHSA-2023:4060)                 |
| 241904 Red Hat Update for .net 6.0 (RHSA-2023:4448)                          |
| 241905 Red Hat Update for .net 6.0 (RHSA-2023:4449)                          |
| 284341 Fedora Security Update for dotnet6.0 (FEDORA-2023-4a48637c3f)         |
| 284342 Fedora Security Update for dotnet6.0 (FEDORA-2023-fed45bc39)          |
| 284343 Fedora Security Update for dotnet7.0 (FEDORA-2023-18264c31f6)         |
| 284344 Fedora Security Update for dotnet7.0 (FEDORA-2023-d25e798d6c)         |
| 355882 Amazon Linux Security Advisory for dotnet6.0 : ALAS2023-2023-302      |
| 503160 Alpine Linux Security Update for dotnet6-build                        |
| 503164 Alpine Linux Security Update for dotnet6-runtime                      |
| 503168 Alpine Linux Security Update for dotnet7-build                        |
| 503173 Alpine Linux Security Update for dotnet7-runtime                      |
| 506004 Alpine Linux Security Update for dotnet6-build                        |
| 506012 Alpine Linux Security Update for dotnet6-runtime                      |
| 506020 Alpine Linux Security Update for dotnet7-build                        |
| 506033 Alpine Linux Security Update for dotnet7-runtime                      |
| 92034 Microsoft Visual Studio Security Updates for July 2023                 |
| 92036 Microsoft .NET Security Update for July 2023                           |
| 941171 AlmaLinux Security Update for .NET (ALSA-2023:4060)                   |

[941172](#) AlmaLinux Security Update for .NET (ALSA-2023:4059)

[941173](#) AlmaLinux Security Update for .NET (ALSA-2023:4058)

[941175](#) AlmaLinux Security Update for .NET (ALSA-2023:4057)

© [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](#)