



# CVE-2022-30184

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

## Summary

<b>CVE</b>	CVE-2022-30184
<b>State</b>	PUBLIC
<b>Assigner</b>	secure@microsoft.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-06-15 22:15:00 UTC
<b>Updated</b>	2023-12-20 22:15:00 UTC
<b>Description</b>	.NET and Visual Studio Information Disclosure Vulnerability.

## Risk And Classification

**Problem Types:** NVD-CWE-noinfo

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Apple</a>	<a href="#">Macos</a>	-	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	35	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	36	All	All	All
Application	<a href="#">Microsoft</a>	<a href="#">.net</a>	6.0.0	-	All	All
Application	<a href="#">Microsoft</a>	<a href="#">.net Core</a>	3.1	-	All	All
Application	<a href="#">Microsoft</a>	<a href="#">Nuget</a>	All	All	All	All
Application	<a href="#">Microsoft</a>	<a href="#">Visual Studio 2019</a>	All	All	All	All
Application	<a href="#">Microsoft</a>	<a href="#">Visual Studio 2019</a>	8.10	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://portal.msrc.microsoft.com">portal.msrc.microsoft.com</a>
[SECURITY] Fedora 35 Update: dotnet3.1-3.1.420-1.fc35 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
[SECURITY] Fedora 36 Update: dotnet3.1-3.1.420-1.fc36 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
[SECURITY] Fedora 35 Update: dotnet3.1-3.1.420-1.fc35 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
[SECURITY] Fedora 36 Update: dotnet3.1-3.1.420-1.fc36 - package-announce - Fedora Mailing-Lists		<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>

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

[159901](#) Oracle Enterprise Linux Security Update for .net core 3.1 security and bugfix update (ELSA-2022-5061)

[159905](#) Oracle Enterprise Linux Security Update for .net 6.0 security and bugfix update (ELSA-2022-5046)

[159935](#) Oracle Enterprise Linux Security Update for .net 6.0 security and bugfix update (ELSA-2022-5050)

[240466](#) Red Hat Update for .net 6.0 (RHSA-2022:5050)

[240468](#) Red Hat Update for .net 6.0 (RHSA-2022:5046)

[240471](#) Red Hat Update for .net core 3.1 (RHSA-2022:5061)

[240483](#) Red Hat Update for .net 6.0 on rhel 7 (RHSA-2022:5047)

[240492](#) Red Hat Update for .net core 3.1 on rhel 7 (RHSA-2022:5062)

[282906](#) Fedora Security Update for dotnet3.1 (FEDORA-2022-cd37732349)

[282907](#) Fedora Security Update for dotnet3.1 (FEDORA-2022-5508547b1e)

[502265](#) Alpine Linux Security Update for dotnet6-build

[502543](#) Alpine Linux Security Update for dotnet6-runtime

[504680](#) Alpine Linux Security Update for dotnet6-build

[504691](#) Alpine Linux Security Update for dotnet6-runtime

[91912](#) Microsoft Visual Studio Security Update for June 2022

[91913](#) Microsoft .NET Security Update for June 2022

[960143](#) Rocky Linux Security Update for .NET (RLSA-2022:5046)

[960148](#) Rocky Linux Security Update for .NET (RLSA-2022:5061)

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

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

