



CVE-2021-31204

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

Summary

CVE	CVE-2021-31204
State	PUBLIC
Assigner	secure@microsoft.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-05-11 19:15:00 UTC
Updated	2023-12-29 00:15:00 UTC
Description	.NET and Visual Studio Elevation of Privilege 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	Fedoraproject	Fedora	32	All	All	All
Operating System	Fedoraproject	Fedora	33	All	All	All
Operating System	Fedoraproject	Fedora	34	All	All	All
Application	Microsoft	.net	5.0	All	All	All
Application	Microsoft	.net	All	All	All	All
Application	Microsoft	.net Core	3.1	All	All	All
Application	Microsoft	.net Core	All	All	All	All
Application	Microsoft	Visual Studio 2019	All	All	All	All
Application	Microsoft	Visual Studio 2019	8.9	All	All	All

References

Reference	Source	Link
[SECURITY] Fedora 33 Update: dotnet5.0-5.0.203-1.fc33 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
FEDORA-2021-a3c205f5b2	FEDORA	lists.fedoraproject.org
[SECURITY] Fedora 34 Update: dotnet3.1-3.1.115-1.fc34 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
[SECURITY] Fedora 33 Update: dotnet3.1-3.1.115-1.fc33 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
[SECURITY] Fedora 32 Update: dotnet3.1-3.1.115-1.fc32 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
[SECURITY] Fedora 34 Update: dotnet5.0-5.0.203-1.fc34 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org

[SECURITY] Fedora 34 Update: dotnet5.0-5.0.203-1.fc34 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
[SECURITY] Fedora 32 Update: dotnet3.1-3.1.115-1.fc32 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
[SECURITY] Fedora 34 Update: dotnet5.0-5.0.203-1.fc34 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
[SECURITY] Fedora 33 Update: dotnet3.1-3.1.115-1.fc33 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
Security Update Guide - Microsoft Security Response Center	N/A	portal.msrc.microsoft.com
[SECURITY] Fedora 33 Update: dotnet5.0-5.0.203-1.fc33 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
[SECURITY] Fedora 32 Update: dotnet5.0-5.0.203-1.fc32 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
[SECURITY] Fedora 34 Update: dotnet3.1-3.1.115-1.fc34 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- [159234](#) Oracle Enterprise Linux Security Update for dotnet5.0 (ELSA-2021-2036)
- [159235](#) Oracle Enterprise Linux Security Update for dotnet3.1 (ELSA-2021-2037)
- [239275](#) Red Hat Update for dotnet3.1 (RHSA-2021:2037)
- [239276](#) Red Hat Update for dotnet5.0 (RHSA-2021:2036)
- [239341](#) Red Hat Update for .NET Core 3.1 on Red Hat Enterprise Linux (RHSA-2021:1547)
- [239342](#) Red Hat Update for .NET 5.0 on Red Hat Enterprise Linux (RHSA-2021:1546)
- [281148](#) Fedora Security Update for dotnet3.1 (FEDORA-2021-c06b64b5ee)
- [281149](#) Fedora Security Update for dotnet3.1 (FEDORA-2021-f25eb9e302)
- [281150](#) Fedora Security Update for dotnet3.1 (FEDORA-2021-13e3bd248f)
- [281151](#) Fedora Security Update for dotnet5.0 (FEDORA-2021-a3c205f5b2)
- [281152](#) Fedora Security Update for dotnet5.0 (FEDORA-2021-d551431950)
- [281153](#) Fedora Security Update for dotnet5.0 (FEDORA-2021-721731dc86)
- [375634](#) Microsoft Visual Studio For Mac Security Update for May 2021
- [91763](#) Microsoft Visual Studio Security Update for May 2021
- [91766](#) Microsoft .NET Core Security Update May 2021
- [940048](#) AlmaLinux Security Update for dotnet5.0 (ALSA-2021:2036)
- [940205](#) AlmaLinux Security Update for dotnet3.1 (ALSA-2021:2037)

© [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](#)