



CVE-2022-41032

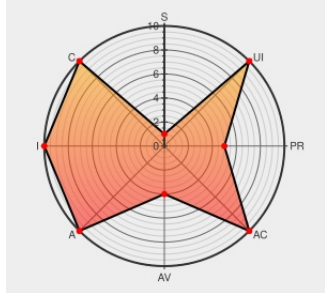
Published on: Not Yet Published

Last Modified on: 12/02/2022 11:00:00 PM UTC

CVE-2022-41032

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

IS:31/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RLO/R



Certain versions of [Fedora](#) from [Fedoraproject](#) contain the following vulnerability:

NuGet Client Elevation of Privilege Vulnerability.

CVE-2022-41032 has been assigned by [secure@microsoft.com](#) to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.8 - HIGH**

Attack
Vector

LOCAL

Attack
Complexity

LOW

Privileges
Required

LOW

User
Interaction

NONE

Scope

UNCHANGED

Confidentiality
Impact

HIGH

Integrity
Impact

HIGH

Availability
Impact

HIGH

CVE References

Description

Tags

Link

Security Update Guide - Microsoft Security Response Center

[portal.msrc.microsoft.com
text/html](https://portal.msrc.microsoft.com/text/html)

[MISC portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41032](https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41032)

[SECURITY] Fedora 35 Update: dotnet3.1-3.1.424-1.fc35 - package-announce - Fedora Mailing-Lists

[lists.fedoraproject.org
text/html](https://lists.fedoraproject.org/text/html)

[FEDORA FEDORA-2022-7f5f9ede26](#)

[SECURITY] Fedora 37 Update: dotnet6.0-6.0.110-2.fc37 - package-announce - Fedora Mailing-Lists

[lists.fedoraproject.org
text/html](https://lists.fedoraproject.org/text/html)

[FEDORA FEDORA-2022-2c37647a9c](#)

[SECURITY] Fedora 36 Update: dotnet3.1-3.1.424-1.fc36 - package-announce - Fedora Mailing-Lists

[lists.fedoraproject.org
text/html](https://lists.fedoraproject.org/text/html)

[FEDORA FEDORA-2022-f9ca76e479](#)

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to

Related QID Numbers

[160139](#) Oracle Enterprise Linux Security Update for .net core 3.1 security and bugfix update (ELSA-2022-6912)

[160140](#) Oracle Enterprise Linux Security Update for .net 6.0 security and bugfix update (ELSA-2022-6913)

[160142](#) Oracle Enterprise Linux Security Update for .net 6.0 security and bugfix update (ELSA-2022-6911)

[160257](#) Oracle Enterprise Linux Security Update for dotnet7.0 (ELSA-2022-7826)

[160333](#) Oracle Enterprise Linux Security Update for dotnet7.0 (ELSA-2022-8434)

[198981](#) Ubuntu Security Notification for .NET 6 Vulnerability (USN-5670-1)

[240724](#) Red Hat Update for .net 6.0 (RHSA-2022:6913)

[240725](#) Red Hat Update for .net core 3.1 (RHSA-2022:6912)

[240726](#) Red Hat Update for .net 6.0 (RHSA-2022:6911)

[240727](#) Red Hat Update for .net 6.0 on rhel 7 (RHSA-2022:6915)

[240728](#) Red Hat Update for .net core 3.1 on rhel 7 (RHSA-2022:6914)

[240859](#) Red Hat Update for dotnet7.0 security (RHSA-2022:7826)

[240915](#) Red Hat Update for dotnet7.0 security (RHSA-2022:8434)

[283237](#) Fedora Security Update for dotnet3.1 (FEDORA-2022-7f5f9ede26)

[283238](#) Fedora Security Update for dotnet3.1 (FEDORA-2022-f9ca76e479)

[283425](#) Fedora Security Update for dotnet6.0 (FEDORA-2022-2c37647a9c)

[502541](#) Alpine Linux Security Update for dotnet6-build

[502542](#) Alpine Linux Security Update for dotnet6-runtime

[91949](#) Microsoft Visual Studio (NuGet Client) Security Update for October 2022

[91950](#) Microsoft .NET (NuGet Client) Security Update for October 2022

[940686](#) AlmaLinux Security Update for .NET (ALSA-2022:6912)

[940688](#) AlmaLinux Security Update for .NET (ALSA-2022:6911)

[940695](#) AlmaLinux Security Update for .NET (ALSA-2022:6913)

[940742](#) AlmaLinux Security Update for dotnet7.0 (ALSA-2022:7826)

[940784](#) AlmaLinux Security Update for dotnet7.0 (ALSA-2022:8434)

[960344](#) Rocky Linux Security Update for .NET (RLSA-2022:6911)

[960362](#) Rocky Linux Security Update for .NET (RLSA-2022:6912)

[960567](#) Rocky Linux Security Update for .NET (RLSA-2022:6913)

Exploit/POC from Github

This repository contains a collection of data files on known Common Vulnerabilities and

This repository contains a collection of data files containing common vulnerabilities and Exposures (CVEs). Each file i...

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	35	All	All	All
Operating System	Fedoraproject	Fedora	36	All	All	All
Operating System	Fedoraproject	Fedora	37	All	All	All
Application	Microsoft	.net	6.0.0	-	All	All
Application	Microsoft	.net Core	3.1	-	All	All
Application	Microsoft	Visual Studio 2019	All	All	All	All
Application	Microsoft	Visual Studio 2022	All	All	All	All
Application	Microsoft	Visual Studio 2022	All	All	All	All
Application	Microsoft	Visual Studio 2022	All	All	All	All
cpe:2.3:o:fedoraproject:fedora:35:*:*:*:*:*:						
cpe:2.3:o:fedoraproject:fedora:36:*:*:*:*:*:						
cpe:2.3:o:fedoraproject:fedora:37:*:*:*:*:*:						
cpe:2.3:a:microsoft:.net:6.0.0:-:*:*:*:*:						
cpe:2.3:a:microsoft:.net_core:3.1:-:*:*:*:*:						
cpe:2.3:a:microsoft:visual_studio_2019:*:*:*:*:*:						
cpe:2.3:a:microsoft:visual_studio_2022:*:*:*:*:*:						
cpe:2.3:a:microsoft:visual_studio_2022:*:*:*:*:*:						
cpe:2.3:a:microsoft:visual_studio_2022:*:*:*:*:macos:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2022-41032 : NuGet Client Elevation of Privilege Vulnerability.... cve.report/CVE-2022-41032	2022-10-11 19:02:58
 /r/netcve	CVE-2022-41032	2022-10-11 20:39:06

[← Previous ID](#)

[Next ID →](#)

© [CVE.report](#) 2023  |

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](#)