



## BULLETIN DE SECURITE

<b>Titre</b>	Vulnérabilités critiques dans plusieurs produits Microsoft (Patch Tuesday Juin 2023)
<b>Numéro de Référence</b>	42381406/23
<b>Date de Publication</b>	14 Juin 2023
<b>Risque</b>	Critique
<b>Impact</b>	Critique

### Systemes affectés

- Microsoft .NET Framework 3.5
- Microsoft .NET Framework 3.5 AND 4.8.1
- Microsoft .NET Framework 4.6.2
- Microsoft .NET Framework 4.6.2/4.7/4.7.1/4.7.2
- Microsoft .NET Framework 3.5 AND 4.8
- Microsoft .NET Framework 4.8
- Azure DevOps Server 2022.0.1
- Microsoft .NET Framework 3.5.1
- Microsoft .NET Framework 3.0 Service Pack 2
- Microsoft .NET Framework 2.0 Service Pack 2
- Microsoft .NET Framework 3.5 and 4.6.2
- Microsoft Visual Studio 2022 version 17.6
- Microsoft .NET Framework 3.5 AND 4.6.2/4.7/4.7.1/4.7.2
- Microsoft .NET Framework 3.5 AND 4.7.2
- .NET 7.0
- .NET 6.0
- Microsoft Visual Studio 2022 version 17.5
- Microsoft Visual Studio 2022 version 17.4
- Microsoft Visual Studio 2022 version 17.0
- Microsoft Visual Studio 2022 version 17.2

- Azure DevOps Server 2022
- Sysinternals Suite
- Windows Sysinternals Process Monitor
- YARP 2.0
- Visual Studio Code
- Azure DevOps Server 2020.1.2
- Microsoft Visual Studio 2019 version 16.11 (includes 16.0 - 16.10)
- Microsoft Visual Studio 2017 version 15.9 (includes 15.0 - 15.8)
- Microsoft Visual Studio 2013 Update 5
- Microsoft Visual Studio 2015 Update 3
- Microsoft Power Apps
- NuGet 6.6.0
- NuGet 6.0.4
- NuGet 6.3.2
- NuGet 6.5.0
- NuGet 6.4.1
- NuGet 6.2.3
- Dynamics 365 for Finance and Operations

### Identificateurs externes

- CVE-2023-24936 , CVE-2023-21569 , CVE-2023-29353 , CVE-2023-29326 , CVE-2023-24895 , CVE-2023-33126 , CVE-2023-33135 , CVE-2023-32020 , CVE-2023-29368 , CVE-2023-32030 , CVE-2023-29372 , CVE-2023-29331 , CVE-2023-29365 , CVE-2023-33141 , CVE-2023-27911 , CVE-2023-33128 , CVE-2023-32032 , CVE-2023-33144 , CVE-2023-21565 , CVE-2023-32011 , CVE-2023-32017 , CVE-2023-29371 , CVE-2023-29359 , CVE-2023-29351 , CVE-2023-29007 , CVE-2023-25652 , CVE-2023-27910 , CVE-2023-33139 , CVE-2023-27909 , CVE-2023-32024 , CVE-2023-29337 , CVE-2023-29362 , CVE-2023-29358 , CVE-2023-29346 , CVE-2023-29012 , CVE-2023-29011 , CVE-2023-25815 , CVE-2023-32016 , CVE-2023-29373 , CVE-2023-29364 , CVE-2023-24896 , CVE-2023-24897 , CVE-2023-32014 , CVE-2023-29363 , CVE-2023-32015

### Bilan de la vulnérabilité

Microsoft annonce la correction de plusieurs vulnérabilités critiques affectant les produits Microsoft susmentionnés. L'exploitation de ces vulnérabilités peut permettre à un attaquant de réussir une élévation de privilèges, d'exécuter du code arbitraire à distance, de porter atteinte à la confidentialité de données, de réussir une usurpation d'identité et de contourner la politique de sécurité.

## **Solution**

Veillez se référer au bulletin de sécurité Microsoft du 13 Juin 2023.

## **Risque**

- Elévation de privilèges
- Exécution du code arbitraire à distance
- Atteinte à la confidentialité de données
- Usurpation d'identité
- Contournement de la politique de sécurité

## **Annexe**

Bulletin de sécurité Microsoft du 13 Juin 2023:

- <https://msrc.microsoft.com/update-guide/fr-FR>