

Agence Nationale
des Systèmes d'information
de l'état

Djibouti le, 11-07-2024

BULLETIN ALERTES

Object	Multiples vulnérabilités dans les produits Microsoft
Référence	1183
Date de Publication	2024-07-11
Sévérité	Critique

IMPACT :

- Élévation de privilèges
- Atteinte à la confidentialité des données
- Déni de service
- Exécution de code à distance

SYSTÈME AFFECTÉ :

- Microsoft Defender pour IoT versions antérieures à 24.1.4
- Microsoft Dynamics 365 (on-premises) version 9.1 antérieures à 9.1.28.09
- Microsoft OLE DB Driver 18 pour SQL Server versions antérieures à 18.7.0004.0
- Microsoft OLE DB Driver 19 pour SQL Server versions antérieures à 19.3.0005.0
- Microsoft SharePoint Enterprise Server 2016 versions antérieures à 16.0.5456.1000
- Microsoft SharePoint Server 2019 versions antérieures à 16.0.10412.20001
- Microsoft SharePoint Server Subscription Edition versions antérieures à 16.0.17328.20424
- Microsoft SQL Server 2016 pour systèmes x64 Service Pack 3 (GDR) versions antérieures à 13.0.6441.1
- Microsoft SQL Server 2016 pour systèmes x64 Service Pack 3 Azure Connect Feature Pack versions antérieures à 13.0.7037.1
- Microsoft SQL Server 2017 pour systèmes x64 (CU 31) versions antérieures à 14.0.3471.2
- Microsoft SQL Server 2017 pour systèmes x64 (GDR) versions antérieures à 14.0.2056.2
- Microsoft SQL Server 2019 pour systèmes x64 (CU 27) versions antérieures à 15.0.4382.1
- Microsoft SQL Server 2019 pour systèmes x64 (GDR) versions antérieures à 15.0.2116.2
- Microsoft SQL Server 2022 pour systèmes x64 (CU 13) versions antérieures à 16.0.4131.2
- Microsoft SQL Server 2022 pour systèmes x64 (GDR) versions antérieures à 16.0.1121.4
- Microsoft Visual Studio 2022 version 17.10 antérieures à 17.10.4
- Microsoft Visual Studio 2022 version 17.4 antérieures à 17.4.21
- Microsoft Visual Studio 2022 version 17.6 antérieures à 17.6.17
- Microsoft Visual Studio 2022 version 17.8 antérieures à 17.8.12

DÉSCRIPTION :

Des nombreuses vulnérabilités ont été découvertes dans les produits Microsoft. L'exploitation de ces vulnérabilités permet à un attaquant de provoquer une atteinte à la confidentialité des données, un déni de service, une élévation de privilèges, une exécution de code arbitraire à distance.

SOLUTION :

Appliquer les correctifs sur vos produit Microsoft. (Se référer à la documentation)

DOCUMENTATION :

- Bulletin de sécurité Microsoft du 09 juillet 2024

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

- CVE-2024-20701

<https://www.cve.org/CVERecord?id=CVE-2024-20701>

- CVE-2024-21303

<https://www.cve.org/CVERecord?id=CVE-2024-21303>

- CVE-2024-21308

<https://www.cve.org/CVERecord?id=CVE-2024-21308>

- CVE-2024-21317

<https://www.cve.org/CVERecord?id=CVE-2024-21317>

- CVE-2024-21331

<https://www.cve.org/CVERecord?id=CVE-2024-21331>

- CVE-2024-21332

<https://www.cve.org/CVERecord?id=CVE-2024-21332>

- CVE-2024-21333

<https://www.cve.org/CVERecord?id=CVE-2024-21333>

- CVE-2024-21335

<https://www.cve.org/CVERecord?id=CVE-2024-21335>

- CVE-2024-21373

<https://www.cve.org/CVERecord?id=CVE-2024-21373>

- CVE-2024-21398

<https://www.cve.org/CVERecord?id=CVE-2024-21398>

- CVE-2024-21414

<https://www.cve.org/CVERecord?id=CVE-2024-21414>

- CVE-2024-21415

<https://www.cve.org/CVERecord?id=CVE-2024-21415>

- CVE-2024-21425

<https://www.cve.org/CVERecord?id=CVE-2024-21425>

- CVE-2024-21428

<https://www.cve.org/CVERecord?id=CVE-2024-21428>

- CVE-2024-21449

<https://www.cve.org/CVERecord?id=CVE-2024-21449>

- CVE-2024-28928

<https://www.cve.org/CVERecord?id=CVE-2024-28928>

- CVE-2024-30061

<https://www.cve.org/CVERecord?id=CVE-2024-30061>

- CVE-2024-30105

<https://www.cve.org/CVERecord?id=CVE-2024-30105>

- CVE-2024-32987

<https://www.cve.org/CVERecord?id=CVE-2024-32987>

- CVE-2024-35256

<https://www.cve.org/CVERecord?id=CVE-2024-35256>

- CVE-2024-35264

<https://www.cve.org/CVERecord?id=CVE-2024-35264>

- CVE-2024-35271

<https://www.cve.org/CVERecord?id=CVE-2024-35271>

- CVE-2024-35272

<https://www.cve.org/CVERecord?id=CVE-2024-35272>

- CVE-2024-37318

<https://www.cve.org/CVERecord?id=CVE-2024-37318>

- CVE-2024-37319

<https://www.cve.org/CVERecord?id=CVE-2024-37319>

- CVE-2024-37320

<https://www.cve.org/CVERecord?id=CVE-2024-37320>

- CVE-2024-37321

<https://www.cve.org/CVERecord?id=CVE-2024-37321>

- CVE-2024-37322

<https://www.cve.org/CVERecord?id=CVE-2024-37322>

- CVE-2024-37323

<https://www.cve.org/CVERecord?id=CVE-2024-37323>

- CVE-2024-37324

<https://www.cve.org/CVERecord?id=CVE-2024-37324>

- CVE-2024-37326

<https://www.cve.org/CVERecord?id=CVE-2024-37326>

- CVE-2024-37327

<https://www.cve.org/CVERecord?id=CVE-2024-37327>

- CVE-2024-37328

<https://www.cve.org/CVERecord?id=CVE-2024-37328>

- CVE-2024-37329

<https://www.cve.org/CVERecord?id=CVE-2024-37329>

- CVE-2024-37330

<https://www.cve.org/CVERecord?id=CVE-2024-37330>

- CVE-2024-37331

<https://www.cve.org/CVERecord?id=CVE-2024-37331>

- CVE-2024-37332

<https://www.cve.org/CVERecord?id=CVE-2024-37332>

- CVE-2024-37333

<https://www.cve.org/CVERecord?id=CVE-2024-37333>

- CVE-2024-37334

<https://www.cve.org/CVERecord?id=CVE-2024-37334>

- CVE-2024-37336

<https://www.cve.org/CVERecord?id=CVE-2024-37336>

- CVE-2024-38023

<https://www.cve.org/CVERecord?id=CVE-2024-38023>

- CVE-2024-38024

<https://www.cve.org/CVERecord?id=CVE-2024-38024>

- CVE-2024-38081

<https://www.cve.org/CVERecord?id=CVE-2024-38081>

- CVE-2024-38087

<https://www.cve.org/CVERecord?id=CVE-2024-38087>

- CVE-2024-38088

<https://www.cve.org/CVERecord?id=CVE-2024-38088>

- CVE-2024-38089

<https://www.cve.org/CVERecord?id=CVE-2024-38089>

- CVE-2024-38094

<https://www.cve.org/CVERecord?id=CVE-2024-38094>

- CVE-2024-38095

<https://www.cve.org/CVERecord?id=CVE-2024-38095>