aDvens

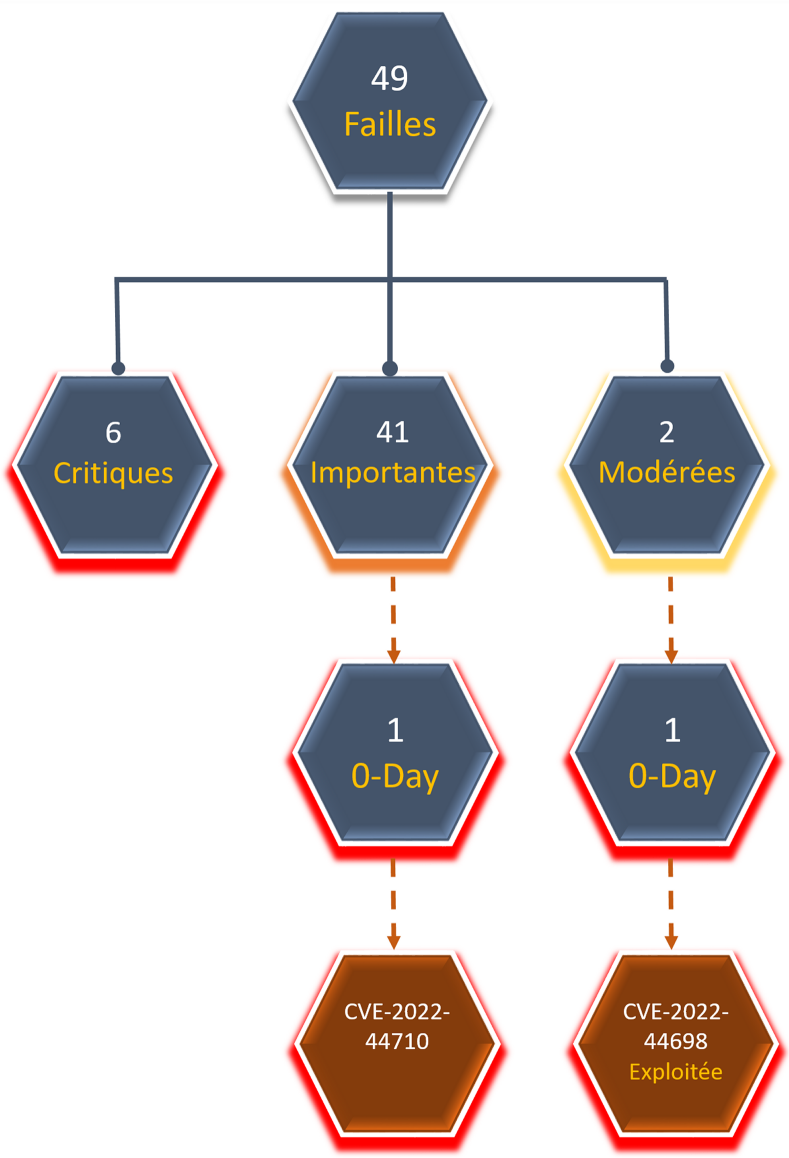
Security for the greater good

Renseignement sur les menaces
Patch Tuesday de décembre 2022

2022-12-14 | **TLP:CLEAR** | CERT aDvens - CTI
Advens - 16 Quai de la Mégisserie - 75001 Paris

Sommaire

1. Synthèse



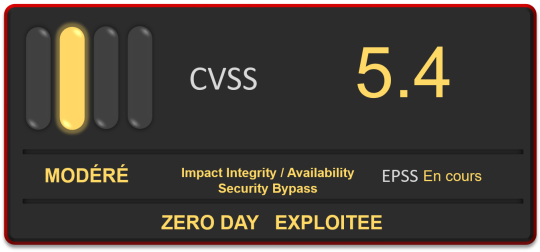
Le mercredi 14 décembre 2022, Microsoft a publié son bulletin mensuel ***Patch tuesday***, avec **49 failles** corrigées dont **2 zero day** et une **activement exploitée** : CVE-2022-44698 (exploitée) et CVE-2022-44710.

Ce document aborde les vulnérabilités, ci-dessous, considérées comme les plus critiques :

PRODUIT	CVE	SCORE	EPSS	ZERO-DAY	EXPLOITEE	CWE	POC
SmartScreen	CVE-2022-44698	5.4 importante	En cours	Oui	Oui	254	Oui
DirectX Graphic	CVE-2022-44710	7.8 importante	En cours	Oui	Non	362	Non
SharePoint	CVE-2022-44690	8.8 critique	En cours	Non	Non	20	Non
SharePoint	CVE-2022-44693	8.8 critique	En cours	Non	Non	20	Non
Dynamics NAV BC	CVE-2022-41127	8.5 critique	En cours	Non	Non	20	Non
PowerShell	CVE-2022-41076	8.5 critique	En cours	Non	Non	20	Non
SSTP	CVE-2022-44670	8.1 critique	En cours	Non	Non	362	Non
SSTP	CVE-2022-44676	8.1 critique	En cours	Non	Non	362	Non

2. SmartScreen CVE-2022-44698 (Zero day - Exploitée)

2.1. Résumé



Étudiée par le chercheur Will Dormann de la société *ANALYGENCE*, cette vulnérabilité est un défaut de sécurité affectant le filtre *SmartScreen*, qui permet de contourner la politique de sécurité MOTW (Mark Of The Web). Un attaquant, distant et non authentifié, peut exploiter cette faille afin de porter atteinte à l'intégrité et la disponibilité des données.

Développé par Microsoft, *SmartScreen* est un filtre anti-phishing et anti-maliciel déployé sur le système d'exploitation Windows et le navigateur Internet Edge.

La fonctionnalité *MoTW* permet de déterminer la provenance d'un fichier par l'intermédiaire d'un *identifiant de zone*, implémenté dans les propriétés du fichier. Pour un fichier provenant d'internet, l'identifiant est 3. L'utilisateur est averti via une fenêtre de sécurité de l'origine de ce fichier et doit valier son ouverture ou exécution.

Cette vulnérabilité est exploitée. Une interaction avec la victime est nécessaire.

Comme mentionné dans le bulletin du CERT aDvens du mois dernier, cette vulnérabilité a été utilisée lors de campagnes récentes pour déployer le cheval de Troie Qbot et le rançongiciel Magniber.

2.2. Informations

2.2.1. Risque

- Atteinte à l'intégrité des données.
- Atteinte à la disponibilité des données.
- Contournement de la politique de sécurité.

2.2.2. Type de vulnérabilité

- **CWE-254**: 7PK - Security Features

2.2.3. Criticité

Vecteur d'attaque: Réseau	Interaction de l'utilisateur: Oui	Impact sur l'intégrité: Faible
Complexité d'attaque: Faible	Portée: Inchangée	Impact sur la disponibilité: Faible
Privilèges requis: Aucun	Impact sur la confidentialité: Aucun	

2.2.4. Composants vulnérables

- Microsoft Windows Server 2012
- Microsoft Windows Server 2016
- Microsoft Windows Server 2019
- Microsoft Windows Server 2022
- Microsoft Windows 8.1
- Microsoft Windows 10
- Microsoft Windows 11

2.2.5. Recommandations

Le patch Tuesday du mois de décembre 2022 apporte les correctifs nécessaires.

Des informations complémentaires sont disponibles sur le site de l'éditeur.

2.2.6. Produits concernés et mises à jour à appliquer

Windows Server 2016

KB5021235

Windows 10 Version 1607 (x32 & x64)

KB5021235

Windows 10 Version 22H2 (x32 / x64 / ARM64)

KB5021233

Windows 10 Version 21H2 (x32 / x64 / ARM64)

KB5021233

Windows 11 (x64 & ARM64)

KB5021234

Windows 10 Version 20H2 (x32 / x64 / ARM64)

KB5021233

Windows Server 2022 Datacenter: Azure Edition

KB5021249

Windows Server 2022

KB5021249

Windows 10 Version 21H1 (x32 : x64 : ARM64)

KB5021233

Windows Server 2019

KB5021237

Windows 10 Version 1809 (x32 / x64 / ARM64)

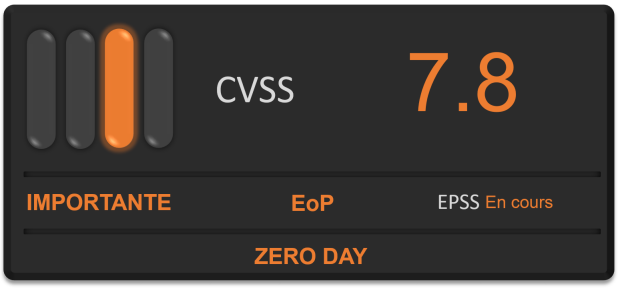
KB5021237

2.2.7. Preuve de concept

Un exploit (POC) est disponible en sources ouvertes.

3. DirectX Graphic Kernel CVE-2022-44710 (Zero day)

3.1. Résumé



Cette vulnérabilité zero-day, localisée dans le noyau *DirectX Graphics*, est un défaut de type *race condition* ou *situation de concurence* qui affecte le système d'exploitation Windows 11.

Une situation de concurrence peut se manifester lorsqu'une ressource est partagée, sans précaution, entre plusieurs tâches.

L'exploitation de cette vulnérabilité permet à un attaquant, authentifié localement en tant que simple utilisateur, d'élever ses privilèges.

3.2. Informations

3.2.1. Risque

- Élévation de privilèges.

3.2.2. Type de vulnérabilité

- **CWE-362**: Concurrent Execution using Shared Resource with Improper Synchronization (*Race Condition*)

3.2.3. Criticité

Vecteur d'attaque: Local	Interaction de l'utilisateur: Non	Impact sur l'intégrité: Fort
Complexité d'attaque: Haute	Portée: Changée	Impact sur la disponibilité: Fort
Privilèges requis: Faible	Impact sur la confidentialité: Fort	

3.2.4. Composants vulnérables

- Windows 11 Version 22H2 (x64 et ARM64)

3.2.5. Recommandations

Le patch Tuesday du mois de décembre 2022 apporte les correctifs nécessaires.

Des informations complémentaires sont disponibles sur le site de l'éditeur.

3.2.6. Produits concernés et mises à jour à appliquer

Windows 11 Version 22H2 (x64 & ARM64)

KB5021255

3.2.7. Preuve de concept

Actuellement, aucun exploit (POC) n'est disponible en sources ouvertes.

4. SharePoint CVE-2022-44690 / 44693

4.1. Résumé

Des chercheurs, en collaboration avec le laboratoire *VCSLAB* de la société *Viettel Cyber Security*, ont identifié deux vulnérabilités qui affectent *Microsoft SharePoint*.

Un contrôle insuffisant des données saisies permet à un attaquant, distant et authentifié avec un compte utilisateur détenant les autorisations *Manage List*, d'exécuter du code arbitraire sur le serveur.

4.2. Informations

4.2.1. Risque

- Exécution de code arbitraire à distance.

4.2.2. Type de vulnérabilité

- **CWE-20**: Improper Input Validation

4.2.3. Criticité

Vecteur d'attaque : Réseau	Interaction de l'utilisateur : Non	Impact sur l'intégrité : Fort
Complexité d'attaque : Faible	Portée : Inchangée	Impact sur la disponibilité : Fort
Privilèges requis : Faible	Impact sur la confidentialité : Fort	

4.2.4. Composants vulnérables

- Microsoft SharePoint Foundation 2013 Service Pack 1
- Microsoft SharePoint Server Subscription Edition
- Microsoft SharePoint Server 2019
- Microsoft SharePoint Enterprise Server 2013 Service Pack 1
- Microsoft SharePoint Enterprise Server 2016

4.2.5. Recommandations

Le patch Tuesday du mois de décembre 2022 apporte les correctifs nécessaires.

Des informations complémentaires pour la CVE-2022-44690 sont disponibles sur le site de l'éditeur.

Des informations complémentaires pour la CVE-2022-44693 sont disponibles sur le site de l'éditeur.

4.2.6. Produits concernés et mises à jour à appliquer

Microsoft SharePoint Foundation 2013 Service Pack 1

KB5002319

Microsoft SharePoint Server Subscription Edition

KB5002327

Microsoft SharePoint Server 2019

KB5002311

Microsoft SharePoint Enterprise Server 2013 Service Pack 1

KB5002319

Microsoft SharePoint Enterprise Server 2016

KB5002321

4.2.7. Preuve de concept

Actuellement, aucun exploit (POC) n'est disponible en sources ouvertes.

5. Dynamics NAV / Business Central CVE-2022-41127

5.1. Résumé

L'expert Yiming Xiang, en collaboration avec le laboratoire *NSFOCUS TIANJI LAB*, ont découvert une vulnérabilité qui affecte deux produits Microsoft: *Dynamics NAV* et *Dynamics 365 Business Central*.

Progiciel de gestion intégré, *Dynamics NAV* permet une gestion complète des processus d'une organisation (production, commerce, projets, services clients, finance…).

Dynamics 365 Business Central est un système spécialisé dans la planification des ressources d'une organisation (chaine d'approvisionnement, manufacture…).

Les chercheurs ont découvert que le traitement des données saisies par l'utilisateur n'est pas contrôlé de manière optimale.

Un défaut de contrôle des données saisies permet à un attaquant distant et authentifié, en forgeant un appel réseau, d'excécuter du code arbitraire sur le système.

L'impact de cette vulnérabilité n'est pas limité à *Dynamics NAV* mais peut s'étendre au système d'exploitation.

5.2. Informations

5.2.1. Risque

- Exécution de code arbitraire à distance.

5.2.2. Type de vulnérabilité

- **CWE-20**: Improper Input Validation

5.2.3. Criticité

Vecteur d'attaque: Réseau	Interaction de l'utilisateur: Non	Impact sur l'intégrité: Fort
Complexité d'attaque: Haute	Portée: Changée	Impact sur la disponibilité: Fort
Privilèges requis: Faible	Impact sur la confidentialité: Fort	

5.2.4. Composants vulnérables

- Dynamics 365 Business Central 2021 Release Wave 1
- Dynamics 365 Business Central 2022 Release Wave 2
- Dynamics 365 Business Central 2021 Release Wave 2
- Dynamics 365 Business Central 2022 Release Wave 1
- Dynamics 365 Business Central 2020 Release Wave 1
- Dynamics 365 Business Central 2020 Release Wave 2
- Dynamics 365 Business Central 2019 Release Wave 2 (On-Premise)
- Dynamics 365 Business Central Spring 2019 Update
- Dynamics NAV 2018
- Dynamics NAV 2017
- Dynamics NAV 2016

5.2.5. Recommandations

Le patch Tuesday du mois de décembre 2022 apporte les correctifs nécessaires.

Des informations complémentaires sont disponibles sur le site de l'éditeur.

5.2.6. Produits concernés et mises à jour à appliquer

Microsoft Dynamics 365 Business Central 2021 Release Wave 1

KB5019239

Microsoft Dynamics 365 Business Central 2022 Release Wave 2

KB5021672

Microsoft Dynamics 365 Business Central 2021 Release Wave 2

KB5021670

Microsoft Dynamics 365 Business Central 2022 Release Wave 1

KB5021671

Microsoft Dynamics 365 Business Central 2020 Release Wave 1

KB5010910

Microsoft Dynamics 365 Business Central 2020 Release Wave 2

KB5013420

Dynamics 365 Business Central 2019 Release Wave 2 (On-Premise)

KB4528706

Dynamics 365 Business Central Spring 2019 Update

KB5021669

Microsoft Dynamics NAV 2018

KB5021668

Microsoft Dynamics NAV 2017

KB5010202

Microsoft Dynamics NAV 2016

KB5005293

5.2.7. Preuve de concept

Actuellement, aucun exploit (POC) n'est disponible en sources ouvertes.

6. PowerShell CVE-2022-41076

6.1. Résumé

Le laboratoire *VCSLAB* de la société *Viettel Cyber Security*, en collaboration avec plusieurs chercheurs, ont étudié un défaut de traitement des données au sein de l'interpréteur de commande *PowerShell*.

Cette étude a mis en évidence un contrôle insuffisant des données saisies, permettant à un attaquant distant et authentifié, de contourner la politique de sécurité et exécuter du code arbitraire sur le système.

Microsoft précise que l'exploitation peut être réalisée quelque soit le niveau de privilèges dont bénéficie l'attaquant.

6.2. Informations

6.2.1. Risque

- Exécution de code arbitraire.
- Contournement de la politique de sécurité.

6.2.2. Type de vulnérabilité

- **CWE-20**: Improper Input Validation

6.2.3. Criticité

Vecteur d'attaque: Réseau	Interaction de l'utilisateur: Non	Impact sur l'intégrité: Fort
Complexité d'attaque: Haute	Portée: Changée	Impact sur la disponibilité: Fort
Privilèges requis: Faible	Impact sur la confidentialité: Fort	

6.2.4. Composants vulnérables

- Microsoft Windows 7
- Microsoft Windows 8.1
- Microsoft Windows 10

- Microsoft Windows 11
- Microsoft Windows Server 2008
- Microsoft Windows Server 2012
- Microsoft Windows Server 2016
- Microsoft Windows Server 2019
- Microsoft Windows Server 2022

Produits dépendants:

- Microsoft PowerShell 7.2
- Microsoft PowerShell 7.3
- Microsoft Windows Server 2022 Datacenter: Azure Edition

6.2.5. Recommandations

Le patch Tuesday du mois de décembre 2022 apporte les correctifs nécessaires.

Des informations complémentaires sont disponibles sur le site de l'éditeur.

6.2.6. Produits concernés et mises à jour à appliquer

Windows Server 2012 R2 (Server Core installation)

KB5021296

Windows Server 2012 R2

KB5021296

Windows Server 2012 (Server Core installation)

KB5021303

Windows Server 2012

KB5021303

Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)

KB5021288

Windows Server 2008 R2 for x64-based Systems Service Pack 1

KB5021288

Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)

KB5021293

Windows Server 2008 for x64-based Systems Service Pack 2

KB5021293

Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)

KB5021293

Windows Server 2008 for 32-bit Systems Service Pack 2

KB5021293

Windows RT 8.1

KB5021294

Windows 8.1 (x32 / x64)

KB5021296

Windows 7 Service Pack 1 (x32 / x64)

KB5021288

Windows Server 2016 (Server Core installation)

KB5021235

Windows Server 2016

KB5021235

Windows 10 Version 1607 (x32 / x64)

KB5021235

Windows 10 (x32 / x64)

KB5021243

Windows 10 Version 22H2 (x32 / x64 / ARM64)

KB5021233

Windows 11 Version 22H2 (x64 / ARM64)

KB5021255

Windows 10 Version 21H2 (x32 / x64 / ARM64)

KB5021233

Windows 11 (x64 / ARM)

KB5021234

Windows 10 Version 20H2 (x32 / x64 / ARM64)

KB5021233

Windows Server 2022 Datacenter: Azure Edition

KB5021249

Windows Server 2022 (Server Core installation)

KB5021249

Windows Server 2022

KB5021249

Windows 10 Version 21H1 (x32 / x64 / ARM64)

KB5021233

Windows Server 2019 (Server Core installation)

KB5021237

Windows Server 2019

KB5021237

Windows 10 Version 1809 (x32 / x64 / ARM64)

KB5021237

PowerShell 7.3

KBRelease Notes

PowerShell 7.2

KBRelease Notes

6.2.7. Preuve de concept

Actuellement, aucun exploit (POC) n'est disponible en sources ouvertes.

7. SSTP CVE-2022-44670 / 44676

7.1. Résumé

Disponible depuis le système d'exploitation Vista, Secure Socket Tunneling Protocol (SSTP) est un type de tunnel VPN dispensant un mécanisme sécurisé pour transporter des trames PPP (Point-to-Point Protocol).

Les chercheurs Yuki Chen et Cyber Kunlun ont identifié deux vulnérabilités au sein de ce protocole, de type *race condition* ou *situation de concurence*.

Une situation de concurrence peut se manifester lorsqu'une ressource est partagée, sans précaution, entre plusieurs tâches.

L'exploitation de cette faille permet à un attaquant distant et non authentifié, via une requête spécifiquement forgée, d'exécuter du code arbitraire sur le serveur.

Microsoft précise que l'exploitation ne peut être accomplie uniquement si **l'attaquant remporte une situation de concurrence**.

7.2. Informations

7.2.1. Risque

- Exécution de code arbitraire à distance.

7.2.2. Type de vulnérabilité

- **CWE-362**: Concurrent Execution using Shared Resource with Improper Synchronization (*Race Condition*)

7.2.3. Criticité

Vecteur d'attaque: Réseau	Interaction de l'utilisateur: Non	Impact sur l'intégrité: Fort
Complexité d'attaque: Haute	Portée: Inchangée	Impact sur la disponibilité: Fort
Privilèges requis: Aucun	Impact sur la confidentialité: Fort	

7.2.4. Composants vulnérables

- Microsoft Windows 7
- Microsoft Windows 8.1
- Microsoft Windows 10
- Microsoft Windows 11
- Microsoft Windows Server
- Microsoft Windows Server 2008
- Microsoft Windows Server 2012
- Microsoft Windows Server 2016
- Microsoft Windows Server 2019
- Microsoft Windows Server 2022

7.2.5. Recommandations

Le patch Tuesday du mois de décembre 2022 apporte les correctifs nécessaires.

Des informations complémentaires pour la CVE-2022-44670 et la CVE-2022-44676 sont disponibles sur le site de l'éditeur.

7.2.6. Produits concernés et mises à jour à appliquer

Windows Server 2012 R2 (Server Core installation)

KB5021296

Windows Server 2012 R2

KB5021296

Windows Server 2012 (Server Core installation)

KB5021303

Windows Server 2012

KB5021303

Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)

KB5021288

Windows Server 2008 R2 for x64-based Systems Service Pack 1

KB5021288

Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)

KB5021293

Windows Server 2008 for x64-based Systems Service Pack 2

KB5021293

Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)

KB5021293

Windows Server 2008 for 32-bit Systems Service Pack 2

KB5021293

Windows RT 8.1

KB5021294

Windows 8.1 (x32 / x64)

KB5021296

Windows 7 (x32 / x64) Service Pack 1

KB5021288

Windows Server 2016 (Server Core installation)

KB5021235

Windows Server 2016

KB5021235

Windows 10 Version 1607 (x32 / 64)

KB5021235

Windows 10 (x32 / x64)

KB5021243

Windows 10 Version 22H2 (x32 / x64 / ARM64)

KB5021233

Windows 11 Version 22H2 (x64 / ARM64)

KB5021255

Windows 10 Version 21H2 (x32 / x64 / ARM64)

KB5021233

Windows 11 (x64 / ARM64)

KB5021234

Windows 10 Version 20H2 (x32 / x64 / ARM64)

KB5021233

Windows Server 2022 Datacenter: Azure Edition

KB5021249

Windows Server 2022 (Server Core installation)

KB5021249

Windows Server 2022

KB5021249

Windows 10 Version 21H1 (x32 / x64 / ARM64)

KB5021233

Windows Server 2019 (Server Core installation)

KB5021237

Windows Server 2019

KB5021237

Windows 10 Version 1809 (x32 / x64 / ARM64)

KB5021237

7.2.7. Preuve de concept

Actuellement, aucun exploit (POC) n'est disponible en sources ouvertes.

8. Références

Articles

- https://www.bleepingcomputer.com/news/microsoft/microsoft-december-2022-patch-tuesday-fixes-2-zero-days-49-flaws/
- https://www.bleepingcomputer.com/news/security/exploited-windows-zero-day-lets-javascript-files-bypass-security-warnings/

SmartScreen CVE-2022-44698

- https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-44698
- https://exchange.xforce.ibmcloud.com/vulnerabilities/240976
- https://www.cybersecurity-help.cz/vdb/SB2022121336

DirectX Graphique CVE-2022-44710

- https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-44710
- https://exchange.xforce.ibmcloud.com/vulnerabilities/241699
- https://www.cybersecurity-help.cz/vdb/SB2022121364

SharePoint Graphic CVE-2022-44690

- https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-44690
- https://exchange.xforce.ibmcloud.com/vulnerabilities/240963
- https://www.cybersecurity-help.cz/vdb/SB2022121381

SharePoint Graphic CVE-2022-44693

- https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-44693
- https://exchange.xforce.ibmcloud.com/vulnerabilities/240966
- https://www.cybersecurity-help.cz/vdb/SB2022121381

Dynamics Graphic CVE-2022-44127

- https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-41127
- https://exchange.xforce.ibmcloud.com/vulnerabilities/240934
- https://www.cybersecurity-help.cz/vdb/SB2022121380

PowerShell CVE-2022-44076

- https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-41076
- https://exchange.xforce.ibmcloud.com/vulnerabilities/240994
- https://www.cybersecurity-help.cz/vdb/SB2022121357

SSTP CVE-2022-44670

- https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-44670

- https://exchange.xforce.ibmcloud.com/vulnerabilities/240999
- https://www.cybersecurity-help.cz/vdb/SB2022121361

SSTP CVE-2022-44676

- https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-44676
- https://exchange.xforce.ibmcloud.com/vulnerabilities/240943
- https://www.cybersecurity-help.cz/vdb/SB2022121361