aDvens

Security for the greater good

Rapport CTI

Patch Tuesday du mois de février 2024

2024-02-15 | **TLP:CLEAR** | CERT aDvens - CTI

Advens - 16 Quai de la Mégisserie - 75001 Paris

aDvens

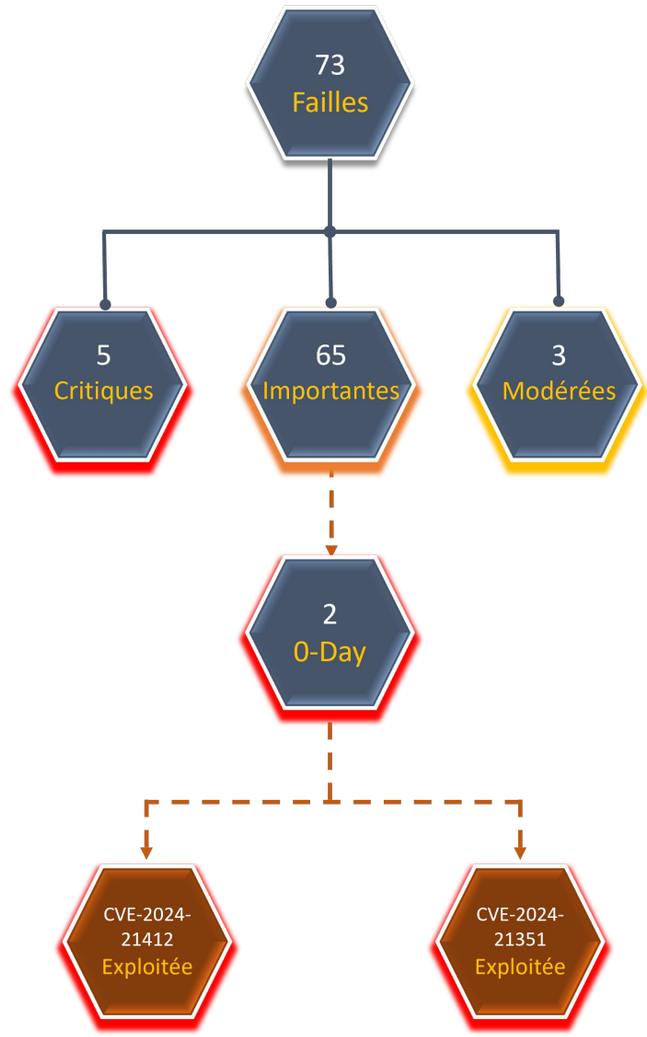
Sommaire

1. Synthèse

Le mardi 13 février 2024, Microsoft a publié son bulletin mensuel ***Patch tuesday***, avec **73 failles** corrigées dont 2 zero-day exploitées : CVE-2024-21412 et CVE-2024-21351.

Le CERT aDvens recommande de tester les mesures de contournement proposées dans un environnement dédié avant leur déploiement en production afin de prévenir tout effet de bord.

Mise à jour du 15 février 2024 : la CVE-2024-21410 (Microsoft Exchange) a été mise à jour suite à l'annonce de Microsoft que celle-ci est exploitée ainsi que la CVE-2024-21413 (Microsoft Office/Outlook) suite à la publication d'une preuve de concept. Le tableau résumé a également été corrigé.



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

PRODUIT	CVE	SCORE	EPSS	ZERO-DAY	EXPLOITEE	CWE	POC
Internet Shortcut	CVE-2024-21412	8.1	1%	Oui	Oui	254	Non
SmartScreen	CVE-2024-21351	7.6	1%	Oui	Oui	254	Non
Exchange	CVE-2024-21410	9.8	0.1%	Non	Oui	668	Non
Office	CVE-2024-21413	9.8	0.1%	Non	Non	20	Oui
Azure AKS	CVE-2024-21403	9.0	0.1%	Non	Non	264	Non

2. Internet Shortcut Files Security - CVE-2024-21412

Cette zero-day exploitée affecte Internet Shortcut Files Security.

Cette faille est due à un défaut de contrôle des liens dans Windows. En persuadant une victime d'ouvrir un fichier spécifiquement forgé contant des liens *Internet Shortcut*, un attaquant peut exploiter cette faille en contournant les contrôles de sécurité afin d'exécuter du code arbitraire.

Une interaction de l'utilisateur est nécessaire.

Cette vulnérabilité serait exploitée depuis décembre 2023. Des chercheurs de *Trend Micro* ont observé au moins deux campagnes exploitant cette vulnérabilité. L'une de ces campagnes, associée au groupe Water Hydra (DarkCasino), cible le secteur financier (*traders*). La deuxième serait associée aux opérateurs de Darkgate. Les attaquants auraient utilisé des mails de phishing contenant un lien vers une image *jpeg* ou un pdf malveillant afin d'exploiter cette vulnérabilité. Lorsque l'utilisateur clique sur l'image, la fenêtre de dialogue d'avertissement des risques potentiels ne s'affichant plus, des fichiers malveillants sont exécutés jusqu'au déploiement du *Remote Access Trojan* DarkMe.

2.1. Type de vulnérabilité

CWE-254 : Security Features

2.2. Risques

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

2.3. Criticité (score de base CVSS v3.1)

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

2.4. Produits impactés

- Windows Server 2019
- Windows Server 2022
- Windows 10
- Windows 11

2.5. Recommandations

Le Patch Tuesday du mois de février 2024 apporte les correctifs nécessaires.

KB5034768

- Windows Server 2019 (Server Core installation)
- Windows Server 2019
- Windows 10 Version 1809 for 32-bit Systems
- Windows 10 Version 1809 for x64-based Systems
- Windows 10 Version 1809 for ARM64-based Systems

5034769

- Windows Server 2022, 23H2 Edition (Server Core installation)

KB5034765

- Windows 11 Version 23H2 for x64-based Systems
- Windows 11 Version 23H2 for ARM64-based Systems
- Windows 11 Version 22H2 for x64-based Systems
- Windows 11 Version 22H2 for ARM64-based Systems

KB5034770

- Windows Server 2022
- Windows Server 2022 (Server Core installation)

KB5034766

- Windows 11 version 21H2 for x64-based Systems
- Windows 11 version 21H2 for ARM64-based Systems

KB5034763

- Windows 10 Version 22H2 for 32-bit Systems
- Windows 10 Version 22H2 for ARM64-based Systems
- Windows 10 Version 22H2 for x64-based Systems
- Windows 10 Version 21H2 for x64-based Systems
- Windows 10 Version 21H2 for ARM64-based Systems
- Windows 10 Version 21H2 for 32-bit Systems

Des informations complémentaires sont disponibles dans le bulletin de Microsoft.

2.6. Preuve de concept

Actuellement, aucune preuve de concept n'est disponible en sources ouvertes.

2.7. Règles de détection

TrendMicro met à disposition les règles suivantes pour détecter l'exploitation de la vulnérabilité.

```
(productCode:sds OR productCode:pds OR productCode:xes OR productCode:sao) AND eventId:1 AND eventSubId:2
AND objectCmd:"rundll32.exe" AND objectCmd:/fxbulls/ AND ( objectCmd:.url OR objectCmd:.cmd)
```

```
(productCode:sds OR productCode:pds OR productCode:xes OR productCode:sao) AND eventId:1 AND eventSubId:2
AND objectCmd:"rundll32.exe" AND objectCmd:/underwall/ AND ( objectCmd:.url OR objectCmd:.cmd)
```

```
eventId:"100101" AND (request:"*84.32.189.74*" OR request:"87iavv.com")
```

```
eventId:3 AND (src:"84.32.189.74*" OR dst:"84.32.189.74*")
```

```
productCode:(pdi OR xns OR pds OR sds OR stp OR ptp OR xcs) AND (eventId:(100115 OR 100119) OR
eventName:INTRUSION_DETECTION) AND (src:"84.32.189.74*" OR dst:"84.32.189.74*")
```

3. Windows SmartScreen - CVE-2024-21351

Cette vulnérabilité, référencé par la CVE-2023-36025, affecte le filtre *SmartScreen* de Windows. Ce filtre permet d'inspecter un fichier en provenance d'internet et disposant du label "*Mark-of-the-Web*".

En persuadant une victime d'ouvrir un fichier spécifiquement forgé, un attaquant peut exploiter cette faille afin d'éviter l'inspection *SmartScreen* et d'exécuter du code arbitraire sur le système.

Une interaction de l'utilisateur est nécessaire.

Cette vulnérabilité est activement exploitée.

3.1. Type de vulnérabilité

- **CWE-254**: Security Features

3.2. Risques

- Contournement de sécurité
- Exécution de code arbitraire

3.3. Criticité (score de base CVSS v3.1)

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

3.4. Produits impactés

- Windows 10
- Windows 11
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022

3.5. Recommandations

Le Patch Tuesday du mois de février 2024 apporte les correctifs nécessaires.

KB5034767

- Windows 10 Version 1607 for 32-bit Systems
- Windows 10 Version 1607 for x64-based Systems

- Windows Server 2016

KB5034774

- Windows 10 for 32-bit Systems
- Windows 10 for x64-based Systems

KB5034763

- Windows 10 Version 21H2 for 32-bit Systems
- Windows 10 Version 21H2 for x64-based Systems
- Windows 10 Version 21H2 for ARM64-based Systems
- Windows 10 Version 22H2 for 32-bit Systems
- Windows 10 Version 22H2 for x64-based Systems
- Windows 10 Version 22H2 for ARM64-based Systems

KB5034765

- Windows 11 Version 22H2 for x64-based Systems
- Windows 11 Version 22H2 for ARM64-based Systems
- Windows 11 Version 23H2 for x64-based Systems
- Windows 11 Version 23H2 for ARM64-based Systems

KB5034766

- Windows 11 version 21H2 for ARM64-based Systems
- Windows 11 version 21H2 for x64-based Systems

KB5034768

- Windows 10 Version 1809 for ARM64-based Systems
- Windows 10 Version 1809 for x64-based Systems
- Windows 10 Version 1809 for 32-bit Systems
- Windows Server 2019

KB5034770

- Windows Server 2022

Des informations complémentaires sont disponibles dans le bulletin de Microsoft.

3.6. Preuve de concept

Actuellement, aucune preuve de concept n'est disponible en sources ouvertes.

4. Microsoft Exchange - CVE-2024-21410

Cette vulnérabilité permet à un attaquant non authentifié, en envoyant des empreintes *Net-NTLMv2* vers un serveur Exchange vulnérable, d'usurper l'identité de l'utilisateur.

Mise à jour du 15 février 2024 : Cette vulnérabilité est activement exploitée.

4.1. Type de vulnérabilité

- **CWE-668** : Exposure of Resource to Wrong Sphere

4.2. Risque

- Contournement d'authentification

4.3. Criticité (score de base CVSS v3.1)

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

4.4. Produits impactés

- Microsoft Exchange Server 2016
- Microsoft Exchange Server 2019

4.4.1. Recommandations

Appliquer les correctifs suivants :

- Microsoft Exchange Server 2016 Cumulative Update 23 et activer la fonctionnalité *Extended Protection* grâce au script ExchangeExtendedProtectionManagement.ps1 de Microsoft
- Microsoft Exchange Server 2019 Cumulative Update 13 et activer la fonctionnalité *Extended Protection* grâce au script ExchangeExtendedProtectionManagement.ps1 de Microsoft
- Microsoft Exchange Server 2019 Cumulative Update 14 : KB5035606

Microsoft a également mis à disposition un article pour aider les administrateurs Exchange à déployer ces correctifs ainsi qu'un script HealthChecker.ps1 pour vérifier que celui-ci a bien été déployé.

Des informations complémentaires sont disponibles dans le bulletin de Microsoft.

4.5. Preuve de concept

Actuellement, aucune preuve de concept n'est disponible en sources ouvertes.

5. Microsoft Office - CVE-2024-21413

Elle permet à un attaquant non authentifié de créer un lien malveillant contournant le protocole *Protected View*. Cela peut entrainer une fuite des empreintes NTLM locales et l'exécution de code arbitraire.

Cette faille peut être exploitée simplement en visualisant un message spécifiquement forgé dans le volet de prévisualisation d'Outlook.

5.1. Type de vulnérabilité

CWE-20 : Improper input validation

5.2. Risque

- Exécution de code arbitraire

5.3. Criticité (score de base CVSS v3.1)

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

5.4. Produits impactés

- Microsoft Office 2016 (64-bit edition)
- Microsoft Office 2016 (32-bit edition)
- Microsoft Office LTSC 2021 for 32-bit editions
- Microsoft Office LTSC 2021 for 64-bit editions
- Microsoft 365 Apps for Enterprise for 64-bit Systems
- Microsoft 365 Apps for Enterprise for 32-bit Systems
- Microsoft Office 2019 for 64-bit editions
- Microsoft Office 2019 for 32-bit editions

5.5. Recommandations

Le Patch Tuesday du mois de février 2024 apporte les correctifs nécessaires.

Il est nécessaire d'appliquer tous les correctifs à Microsoft Office 2016 afin de ne plus être vulnérable.

KB5002537, KB5002467, KB5002522, KB5002519 **et** 5002469

- Microsoft Office 2016 (64-bit edition)
- Microsoft Office 2016 (32-bit edition)

Correctif Microsoft Office

- Microsoft Office LTSC 2021 for 32-bit editions
- Microsoft Office LTSC 2021 for 64-bit editions
- Microsoft Office 2019 for 64-bit editions
- Microsoft Office 2019 for 32-bit editions
- Microsoft 365 Apps for Enterprise for 64-bit Systems
- Microsoft 365 Apps for Enterprise for 32-bit Systems

Des informations complémentaires sont disponibles dans le bulletin de Microsoft.

5.6. Preuve de concept

Mise à jour du 15 février 2024 : Une preuve de concept est disponible en sources ouvertes.

6. Azure Kubernetes - CVE-2024-21403

Découverte par le chercheur en sécurité *Yuval Avrahami*, cette vulnérabilité affecte la fonctionnalité Confidential Container de Microsoft Azure Kubernetes Service (AKS).

Confidential Container est une fonctionalité d'AKS, disponible en mode *preview*, qui chiffre les données du conteneur au niveau *Hardware*.

Cette faille permet à un attaquant non authentifié sur le cluster *AKS*, en déplaçant des *Confidential Containers*, de porter atteinte à la confidentialité, l'intégrité et la disponibilité des données.

L'attaquant doit contrôler au préalable une machine du cluster.

6.1. Type de vulnérabilité

- **CWE-264** : Permissions, Privileges, and Access Controls

6.2. Risque

- Contournement de sécurité

6.3. Criticité (score de base CVSS v3.1)

Vecteur d'attaque	Réseau	Portée	Changée
Complexité d'attaque	Elevée	Impact sur la confidentialité	Élevé
Privilèges requis	Aucun	Impact sur l'intégrité	Élevé
Interaction de l'utilisateur	Aucune	Impact sur la disponibilité	Élevé

6.4. Produits impactés

- Azure Kubernetes Service Confidential Containers

6.5. Recommandations

Appliquer les mises à jour Azure du 6 février 2024 et installer **az confcom** versions 0.3.3 ou ultérieures :

- Si **az confcom** n'est pas installé, télécharger la nouvelle version en exécutant la commande **az extension add -n confcom**.
- Si **az confcom** est déjà installé, le mettre à jour en exécutant la commande **az extension add -n confcom**.

6.6. Preuve de concept

Actuellement, aucune preuve de concept n'est disponible en sources ouvertes.

7. Indicateurs de compromission (CVE-2024-21412)

TLP	TYPE	VALEUR	COMMENTAIRE
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74	
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74/xampp/	
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74/webdav/	
TLP:CLEAR	URL	hxxps://fxbulls[.]ru	
TLP:CLEAR	URL	hxxps://fxbulls[.]ru/wp-content/uploads	
TLP:CLEAR	URL	hxxps://fxbulls[.]ru/wp-content/uploads/2023/12/photo_2023-12-29[.]jpg[.]htm	
TLP:CLEAR	URL	hxxps://fxbulls[.]ru/wp-content/uploads/2023/12/photo_2023-12-29[.]jpg[.]html	
TLP:CLEAR	URL	hxxps://84[.]32[.]189[.]74@0[.]0[.]0[.]80/fxbulls/net/2[.]url	
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74/fxbulls	
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74/fxbulls/pictures	
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74/fxbulls/pictures/photo_2023-12-29[.]jpg[.]url	
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74/fxbulls/pictures/Thumbs[.]db	
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74/fxbulls/pictures/2[.]url	
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74/fxbulls/pictures/a2[.]zip	
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74/fxbulls/pictures/a2[.]zip/a2[.]cmd	
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74/fxbulls/pictures/a2[.]zip	
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74/fxbulls/pictures/b3[.]dll	
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74/fxbulls/pictures/7z[.]dll	
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74/fxbulls/pictures/7z[.]exe	
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74/fxbulls/pictures/photo_2023-12-29s[.]jpg	
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74/fxbulls/pictures/My2[.]zip	
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74/fxbulls	
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74/fxbulls/images	
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74/fxbulls/images/photo_2023-12-29[.]jpg[.]url	
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74/fxbulls/images/Thumbs[.]db	
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74/fxbulls/images/2[.]url	

TLP	TYPE	VALEUR	COMMENTAIRE
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74/fxbulls/images/a2[.]zip	
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74/fxbulls/images/a2[.]zip/a2[.]cmd	
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74/fxbulls/images/a2[.]zip	
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74/fxbulls/images/b3[.]dll	
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74/fxbulls/images/7z[.]dll	
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74/fxbulls/images/7z[.]exe	
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74/fxbulls/images/photo_2023-12-29s[.]jpg	
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74/fxbulls/images/My2[.]zip	
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74/fxbulls/net	
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74/fxbulls/net/photo_2023-12-29[.]jpg[.]url	
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74/fxbulls/net/Thumbs[.]db	
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74/fxbulls/net/2[.]url	
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74/fxbulls/net/a2[.]zip	
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74/fxbulls/net/a2[.]zip/a2[.]cmd	
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74/fxbulls/net/a2[.]zip	
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74/fxbulls/net/b3[.]dll	
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74/fxbulls/net/7z[.]dll	
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74/fxbulls/net/7z[.]exe	
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74/fxbulls/net/photo_2023-12-29s[.]jpg	
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74/fxbulls/net/My2[.]zip	
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74/underwall/docs	
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74/underwall/docs/7z.zip	
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74/underwall/docs/passport.jpg.url	
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74/underwall/docs/warop.url	
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74/underwall/expand	
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74/underwall/expand/7z.zip	
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74/underwall/expand/photo_2023-12-26.jpg.url	

TLP	TYPE	VALEUR	COMMENTAIRE
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74/underwall/expand/warop.url	
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74/underwall/society	
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74/underwall/society/7z.zip	
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74/underwall/society/photo_2023-12-26.jpg.url	
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74/underwall/society/warop.url	
TLP:CLEAR	Domaine	fxbulls[.]ru	
TLP:CLEAR	Domaine	87iavv[.]com	
TLP:CLEAR	Domaine	unfawjelesst322[.]com	
TLP:CLEAR	Domaine	p2oaviwt39ui[.]com	
TLP:CLEAR	IP	84[.]32[.]189[.]74	
TLP:CLEAR	IP	179[.]43[.]172[.]127	
TLP:CLEAR	IP	179[.]43[.]172[.]191	
TLP:CLEAR	IP	64[.]31[.]63[.]70	
TLP:CLEAR	IP	64[.]31[.]63[.]194	
TLP:CLEAR	SHA-256	1458a762332676f7807ab45f8f236c22a1a7bb0c21fcd8c779f972f2446a11d0	Trojan.HTML.CVE202421412.A
TLP:CLEAR	SHA-256	758c6364ab560fbeff2bfa8712a2e09132d85d0bf6918e6acc79fe12f5b71ec3	Trojan.HTML.CVE202421412.A
TLP:CLEAR	SHA-256	77d685e29c3dbe75fa8a82c69c68c731a09904020a76145ca27aeaf0058455cd	Trojan.HTML.CVE202421412.A
TLP:CLEAR	SHA-256	b36dc329a5dc766c2645d5f5b6cdaa9542ec3b0aa1bc13dc1f899ce6d95d59fb	Trojan.HTML.CVE202421412.A
TLP:CLEAR	SHA-256	d895fff3c909ea2eb6624fc5f154c924fe0af51c6c899fd9093dc3cd27a5dad2	Trojan.HTML.CVE202421412.A
TLP:CLEAR	SHA-256	008e57d62caa8cfa991f5519eabe3f15d79799b81ba8cc6b67cde6da0dbffdab	Trojan.Win32.CVE202421412.A
TLP:CLEAR	SHA-256	087878208755420d5d7ae2eb6a84482768cb8972732911ac16096cd0c95fa0f7	Trojan.Win32.CVE202421412.A
TLP:CLEAR	SHA-256	1115e4bed3949493d8ab184e5c42f047355f13b9bf91c1621acb7971a148bea2	Trojan.Win32.CVE202421412.A
TLP:CLEAR	SHA-256	18b1dc2e00245cb017ebdedfe63881929d7542eeffa8f42ee0ad20cc2ebf181a	Trojan.Win32.CVE202421412.A
TLP:CLEAR	SHA-256	1956bcd3df47e76b2e9f396514f072311563d092ae02509f817c488567749998	Trojan.Win32.CVE202421412.A
TLP:CLEAR	SHA-256	1fbc621a71578cb22d4e3a0feec68735321358a3aeb18adbe4a20630c7f788b8	Trojan.Win32.CVE202421412.A
TLP:CLEAR	SHA-256	39fb9fb06910f1133f3b23c523a5139f61d243380802b0670a664473d00e1fa9	Trojan.Win32.CVE202421412.A
TLP:CLEAR	SHA-256	3e420ce1dc1a8503f48815b880381dd23206e08be2474d151f1353df7df2d796	Trojan.Win32.CVE202421412.A
TLP:CLEAR	SHA-256	4201ab8c0c4cf0f01f5a25d8e4e7221634776b5bad8c3faad5ad819ec58619ad	Trojan.Win32.CVE202421412.A
TLP:CLEAR	SHA-256	58b0f5da4a53e956b35e77f55ced641291a596e16067b1dab6ac54d9cb6a52a5	Trojan.Win32.CVE202421412.A
TLP:CLEAR	SHA-256	5b16ac1edb747053ee5a085ab826c61218c5b471eaa04f2471dc2e80b5621023	Trojan.Win32.CVE202421412.A

TLP	TYPE	VALEUR	COMMENTAIRE
TLP:CLEAR	SHA-256	5c85a0fe230d351b35da364c797cc95557f5dcceec034eb648e1805237c7203b	Trojan.Win32.CVE202421412.A
TLP:CLEAR	SHA-256	5f4ef55201080ef3a62b0fbdc4c27e0ccdf4041f41c04471f35b127ff6515405	Trojan.Win32.CVE202421412.A
TLP:CLEAR	SHA-256	61de01bc154b1118caacfed3839c996a795d6c21c2efbf1da6b926414f5d182d	Trojan.Win32.CVE202421412.A
TLP:CLEAR	SHA-256	65cc5594b307c2ac4e3c251aeae68dedf7d1f24ba3b0d7ab5ad3623e8a9fc865	Trojan.Win32.CVE202421412.A
TLP:CLEAR	SHA-256	6793e0fbc2def9173bf8e2a6c1aa357ba7fc3e32dc1cf81107677166f175c890	Trojan.Win32.CVE202421412.A
TLP:CLEAR	SHA-256	6bec457f83d0d98f6f6ea1243c2327e012db38fb61680f6bd68dbab0dc07170a	Trojan.Win32.CVE202421412.A
TLP:CLEAR	SHA-256	7058ae0f02e116b38536ee1ec20f47645aecf761361b5a5e85de2961f3cc88c6	Trojan.Win32.CVE202421412.A
TLP:CLEAR	SHA-256	70b4c2d696a24a5ae2f5e5095dc44e68b4605e4690c8a49930194ee87eb80252	Trojan.Win32.CVE202421412.A
TLP:CLEAR	SHA-256	73922ab0d048b45a01f13ba967f1423bc6cd6cc711f8e7d00a4cf2b1d3646f4e	Trojan.Win32.CVE202421412.A
TLP:CLEAR	SHA-256	761fa42bc4cc5332a640c7389240324242981176ca1626e4267cc8a00cf9545f	Trojan.Win32.CVE202421412.A
TLP:CLEAR	SHA-256	88bb1df99e02021801b08beeff87ec3ceb9e16c42f62904c5ac04c1a26213a48	Trojan.Win32.CVE202421412.A
TLP:CLEAR	SHA-256	941cf63028bf8314bc7114a088f4d1f1dd995bec4a4b7c51fda34fbb3528667f	Trojan.Win32.CVE202421412.A
TLP:CLEAR	SHA-256	a45e0ea5a17ba6f3a2ce7258f6cc81c6f93f37873b49218a25ec638987da6f96	Trojan.Win32.CVE202421412.A
TLP:CLEAR	SHA-256	a5096c4624a523a660242e3451c2f4d644431a35098e36b724fab9f7d88d145d	Trojan.Win32.CVE202421412.A
TLP:CLEAR	SHA-256	a9633da58719f07159702101474b6ba78f2ffee28b3f7ebda3feb36db4e2d0e9	Trojan.Win32.CVE202421412.A
TLP:CLEAR	SHA-256	b0ab19986ab1297870854980f1287f1a4b8d003c540773a6c04fb3565e5701ee	Trojan.Win32.CVE202421412.A
TLP:CLEAR	SHA-256	b350a787c19a756c0824e14eec7e9d746450d1aafb28a5d15209ec9f34c58129	Trojan.Win32.CVE202421412.A
TLP:CLEAR	SHA-256	b738e92afc95cba819aa7aebfad459de38743c478e9e8b8f29f9919697b495b0	Trojan.Win32.CVE202421412.A
TLP:CLEAR	SHA-256	b8b6b6d98b7ea689f0c33d55a06afcf20482b25c51929ca9a1b302374290b337	Trojan.Win32.CVE202421412.A
TLP:CLEAR	SHA-256	babbd9c94dedb94be8baac2ddc5b4714c44a8d0c60d49c0dc91708784bc0d57f	Trojan.Win32.CVE202421412.A
TLP:CLEAR	SHA-256	bbdf52481bd1a15710d75b89240c7a360450e2f4f00ba2cb140affba79ebec94	Trojan.Win32.CVE202421412.A
TLP:CLEAR	SHA-256	c86ba0da732e1fa1f06549d3ebc5ae6ae091199e95930681ac2a9152a8834184	Trojan.Win32.CVE202421412.A
TLP:CLEAR	SHA-256	d6000a19198b8b9719fc17f7c06366e542802a8e7e232ba731b72c31226cc890	Trojan.Win32.CVE202421412.A
TLP:CLEAR	SHA-256	d81e7d95004441ea4f5344215232db57f48579bf335c7ba4ed7f6ec6f9136ed0	Trojan.Win32.CVE202421412.A
TLP:CLEAR	SHA-256	db1bc70c0d0c7121f1d4422a6fcd0e0668d9da786affb52dd77852641e425710	Trojan.Win32.CVE202421412.A
TLP:CLEAR	SHA-256	ddda5737b2c3207d72d728bf40709a7296c31e7c50951dcad441f4707581ccb1	Trojan.Win32.CVE202421412.A

TLP	TYPE	VALEUR	COMMENTAIRE
TLP:CLEAR	SHA-256	e1b903eba88b920909876442306e1160eed9b69c69a05ea370cba2121e305ba1	Trojan.Win32.CVE202421412.A
TLP:CLEAR	SHA-256	e49a7d9083b2e448274d117405c39b0c1b2c0c20ab5195bdf94aaeda7cc113d7	Trojan.Win32.CVE202421412.A
TLP:CLEAR	SHA-256	f44964c8fdf6dbdb21c141df61b45467bba5a4482f7ab19fd6f1841fdb791f2a	Trojan.Win32.CVE202421412.A
TLP:CLEAR	SHA-256	f6b01df60d526f1de530230724d41b482adfff81084a1872bb97c316b76e45e3	Trojan.Win32.CVE202421412.A
TLP:CLEAR	SHA-256	f701f500d348b63f3250239cd8305a8b38230e67d74456f3333c6efeeef85bbb	Trojan.Win32.CVE202421412.A
TLP:CLEAR	SHA-256	fb67be10a5a8b26ca86f8f79935ddd4a5b40379bb6d0af21d23f56af14bb2a90	Trojan.Win32.CVE202421412.A
TLP:CLEAR	SHA-256	4307a067db6b6abd852441e6d70de29c3bd0e4d6a68f0449b403401518b7e037	Trojan.Win32.CVE202421412.B
TLP:CLEAR	SHA-256	69fc5bed55acf559035f2c5550bf8807236b580f8e2db88966b3fc80c83914d3	Trojan.Win32.CVE202421412.B
TLP:CLEAR	SHA-256	4c43b4575063d50ca5668e45a434aaf288970c89e8a4414812560ee787307f58	Trojan.Win32.CVE202421412.B
TLP:CLEAR	SHA-256	135cfefe353ca57d24cfb7326f6cf99085f8af7d1785f5967b417985e8a1153c	Trojan.Win32.DARKME.A
TLP:CLEAR	SHA-256	252351cb1fb743379b4072903a5f6c5d29774bf1957defd9a7e19890b3f84146	Trojan.Win32.DARKME.A
TLP:CLEAR	SHA-256	594e7f7f09a943efc7670edb0926516cfb3c6a0c0036ac1b2370ce3791bf2978	Trojan.Win32.DARKME.A
TLP:CLEAR	SHA-256	6e825a6eb4725b82bd534ab62d3f6f37082b7dbc89062541ee1307ecd5a5dd49	Trojan.Win32.DARKME.A
TLP:CLEAR	SHA-256	71d0a889b106350be47f742495578d7f5dbde4fb36e2e464c3d64c839b1d02bc	Trojan.Win32.DARKME.A
TLP:CLEAR	SHA-256	b69d36e90686626a16b79fa7b0a60d5ebfd17de8ada813105b3a351d40422feb	Trojan.Win32.DARKME.A
TLP:CLEAR	SHA-256	bf9c3218f5929dfeccbbdc0ef421282921d6cbc06f270209b9868fc73a080b8c	Trojan.Win32.DARKME.A
TLP:CLEAR	SHA-256	dc1b15e48b68e9670bf3038e095f4afb4b0d8a68b84ae6c05184af7f3f5ecf54	Trojan.Win32.DARKME.A

8. Références

- https://www.zerodayinitiative.com/blog/2024/2/13/the-february-2024-security-update-review
- https://www.bleepingcomputer.com/news/microsoft/microsoft-february-2024-patch-tuesday-fixes-2-zero-days-73-flaws/

Microsoft Internet Shortcut Files Security - CVE-2024-21412

- https://www.trendmicro.com/en_us/research/24/b/cve202421412-water-hydra-targets-traders-with-windows-defender-s.html
- https://www.zerodayinitiative.com/blog/2024/2/13/the-february-2024-security-update-review
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21412
- https://www.cve.org/CVERecord?id=CVE-2024-21412
- https://thecyberexpress.com/cisa-flags-2-critical-windows-vulnerabilities/

Windows SmartScreen - CVE-2024-21351

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21351
- https://www.cve.org/CVERecord?id=CVE-2024-21351

Microsoft Exchange - CVE-2024-21410

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21410
- https://www.cve.org/CVERecord?id=CVE-2024-21410
- https://thehackernews.com/2024/02/critical-exchange-server-flaw-cve-2024.html

Microsoft Outlook - CVE-2024-21413

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21413
- https://www.cve.org/CVERecord?id=CVE-2024-21413

Azure Kubernetes - CVE-2024-21403

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21403
- https://www.cve.org/CVERecord?id=CVE-2024-21403