

Module yuno

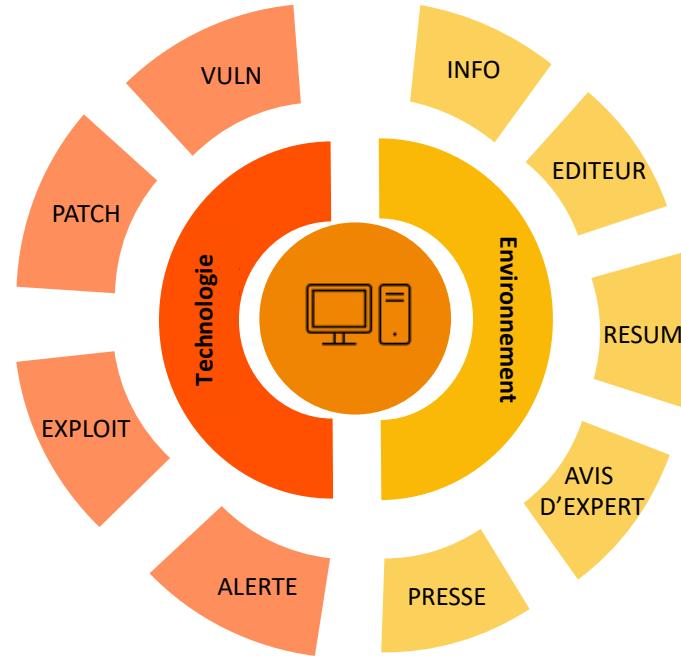
By **xmco**

Gestion de votre veille cyber-sécurité

yuno : Une veille 360° de votre actualité cyber

Le SI de mon client est toujours à jour

Je sais quelle vulnérabilité adresser en priorité



J'ai une vision globale des menaces cyber

Je sensibilise en interne sur les problématiques de sécurité



Veille quotidienne



Veille qualifiée et exploitable



Veille personnalisable



Consultation multi-canal (API, Mailing, SaaS)



Aide à la remédiation dédiée (plan d'action)

Types de bulletins

Deux types de veille sont proposés par le CERT-XMCO.

La veille « technique »

Les bulletins sont associés à des produits/technologies :

- la découverte de vulnérabilités ;
- la publication de correctifs ;
- la publication de codes d'exploitation.



[PATCH] [SAMBA] Prise de contrôle du système via une vulnérabilité au sein de Samba



01/02/2022

Out-of-bounds heap read/write vulnerability in VFS module vfs_fruit allows code execution

Criticité



Dommage

Prise de contrôle d'un système

Plateforme

Indépendant

Exploitation

Distante

Produit concerné

Samba

Français

Anglais

Description

Une vulnérabilité a été corrigée au sein de Samba. Son exploitation permettait à un attaquant de prendre le contrôle du système.

La faille de sécurité référencée [CVE-2021-44142](#) provenait d'une erreur dans le traitement des métadonnées [EA](#) à l'ouverture d'un fichier dans [smbd](#). Un attaquant distant pouvant modifier ces métadonnées pouvait exploiter cette vulnérabilité afin de réaliser des opérations de lecture et d'écriture en dehors des limites prévues sur le tas pour exécuter du code arbitraire avec les priviléges [root](#).

Note : cette vulnérabilité impactait la configuration par défaut du module [vfs_fruit](#) de Samba. Si les options [fruit:metadata](#) et [fruit:resource](#) ont toutes les deux des valeurs différentes que celles par défaut (respectivement [fruit:metadata=netatalk](#) et [fruit:resource=file](#)), alors le serveur n'est pas vulnérable. Cette opération provoque la [perte des données](#) stockées...

La veille « environnementale »



Les bulletins ne sont pas associés à des produits/technologies. Ils traitent de :

- l'actualité de la cyber-sécurité ;
- les publications de chercheurs ;
- les campagnes d'attaques en cours ;
- les bulletins managériaux du CERT-XMCO ;
- ...

[INFO] Deux vulnérabilités sur le logiciel CWP permettent à un attaquant d'exécuter du code à distance sur des serveurs Linux



02/02/2022

Fuite d'informations

Vulnérabilité

CWP bugs allow code execution as root on Linux servers, patch now

Criticité



Français

Anglais

Description

Le 22 janvier dernier, un chercheur en sécurité de [Octagon Networks](#) a identifié deux vulnérabilités permettant à un attaquant d'exécuter du code arbitraire à distance, en tant qu'utilisateur [root](#), sur un serveur Linux.

Les vulnérabilités concernent le logiciel [Control Web Panel](#) (CWP), anciennement appelé [CentOS Web Panel](#), conçu pour gérer des serveurs d'hébergement web dédiés et des serveurs privés virtuels (VPS).

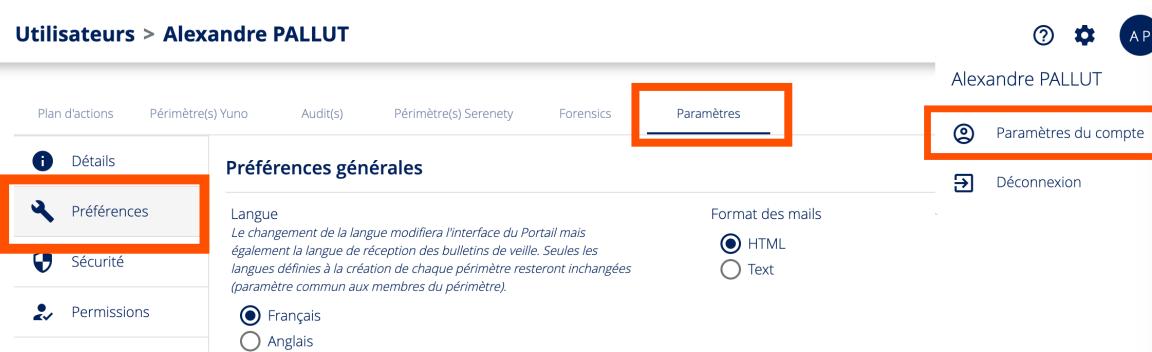
Les deux failles, référencées [CVE-2021-45467](#) et [CVE-2021-45466](#), permettent la lecture (pour la première) et l'écriture (pour la seconde) de fichiers conduisant, lorsqu'elles sont combinées, à une exécution de code arbitraire.

Bien qu'un correctif ait été publié pour la première vulnérabilité, [Octagon Networks](#) affirme qu'il est possible de contourner la solution apportée.

De plus, même si le site de CWP affirme que seuls 30 000 serveurs sont concernés par les failles, des chercheurs en ont identifié plus de 200 000.

Configurer les paramètres de réception

Utilisateurs > Alexandre PALLUT



Plan d'actions Périmètre(s) Yuno Audit(s) Périmètre(s) Serenity Forensics Paramètres

Détails Préférences Sécurité Permissions

Préférences générales

Langue
Le changement de la langue modifiera l'interface du Portail mais également la langue de réception des bulletins de veille. Seules les langues définies à la création de chaque périmètre resteront inchangées (paramètre commun aux membres du périmètre).

Format des mails
 HTML Text

Français Anglais

Étape 2

Définir les paramètres relatifs à la veille technique et environnementale



Veille environnementale

Choisissez de recevoir tous les bulletins de veille environnementale, ou utiliser les filtres pour restreindre les bulletins par criticité, par type, ou par thématiques (tags) spécifiques.

Veille technique

Choisissez de recevoir tous les bulletins de veille technique, ou choisissez de ne recevoir uniquement les bulletins concernant vos périmètres. Vous devrez alors faire partie d'au moins 1 périmètre pour pouvoir recevoir des bulletins techniques.

Étape 1
Cliquez sur le menu en haut à droite, puis Paramètres du compte et enfin Préférences.

Yuno

Réception des bulletins de veille :

- Bulletins individuels
 Synthèse quotidienne des bulletins
 Ne pas recevoir de bulletins

Recevoir les alertes critiques par SMS

- Oui
 Non

Veille informationnelle

Réception de la veille informationnelle :

- Tout recevoir
 Filtrée

Recevoir les bulletins de type :

INFO, XMCO

Recevoir les bulletins de criticité :

Aucune, Faible, Moyenne, Élevée, Critique

Réception des bulletins de type INFO :

- Pas de filtrage par tag
 Filtrer sur les tags suivants:

Reception des bulletins de type XMCO :

- Pas de filtrage par tag
 Filtrer sur les tags suivants:

Tags

Tags

Veille technique

Réception de la veille technique

- Tout recevoir
 Appliquer les paramètres relatifs à mes périmètres

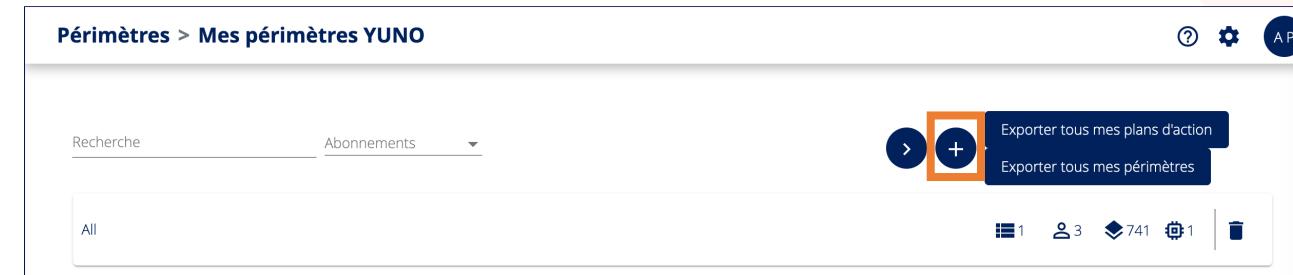
Annuler

Mettre à jour

Créer un périmètre

Étape 1

Cliquez sur Mes Périmètres



Étape 2

Ajouter un périmètre

Ajout d'un périmètre

Nom du périmètre *

Abonnement *

Propriétaire *

Périmètre parent

Description

Accès au périmètre Lecture seule Lecture et écriture

Utilisateur(s)

Annuler Ajouter

Étape 3

Renseignez les champs proposés et cliquez sur **ajouter** pour confirmer l'ajout.

Les utilisateurs ajoutés au périmètre recevront les bulletins concernant les technologies associées à ce périmètre.

Les utilisateurs désignés avec un accès en mode « lecture/écriture » seront en mesure de supprimer une technologie ou d'en ajouter de nouvelles. Cette action ne sera pas possible pour un utilisateur en mode « lecture seule ».



Un **périmètre** est un regroupement de **technologies et d'utilisateurs** qui souhaitent les surveiller.

Ajouter des technologies à suivre dans un périmètre

Étape 1

Cliquez sur Mes Périmètres



Étape 2

Sélectionnez le périmètre à modifier



Étape 3

Vous pouvez accéder à la liste des technologies associées à votre périmètre via l'onglet « Technologies Déployées ».



Étape 4

Cliquez ici pour ajouter ou supprimer une ou plusieurs technologies.

Ajouter des utilisateurs dans un périmètre

Étape 1

Cliquez sur Mes Périmètres



Périmètres > Mes périmètres YUNO

Recherche Abonnements

All

architecture OS

Base de données

Exporter tous mes plans d'action
Exporter tous mes périmètres

1	3	741	1	
0	5	3	0	
73	0	3	0	



Étape 2

Sélectionnez le périmètre à modifier

Périmètres > infra

Plan d'actions Technologie(s) déployée(s) Composant(s) Technique(s) Statistiques Utilisateur(s)

Recherche Profils Activation du compte Langue du compte

Appliquer

Les utilisateurs disposent du droit de lecture sur le périmètre. Le droit d'écriture peut être accordé au cas par cas.

USER Yuno

Login : apallut+test1@xmco.fr
Profils : Manager Serenity, Manager Veille, manager

0 0 2 0

Droit d'écriture sur ce périmètre

Étape 3
Cliquez sur l'onglet Utilisateurs

Étape 4
Cliquez ici pour ajouter ou supprimer des utilisateurs.

Configurer les filtres de réception pour un périmètre

Étape 1

Cliquez sur Mes Périmètres



Plan d'actions Technologie(s) déployée(s) Composant(s) Technique(s) Statistiques Utilisateur(s) Détails Préférences

Cette page vous permet de gérer les options de réception des bulletins Yuno et de génération des tickets d'action associés aux technologies implémentées au sein de vos périmètres. Ces technologies peuvent être spécifiées lors de l'ajout d'un "Composant Technique" à votre périmètre d'audit. Dès lors, les bulletins Yuno publiés chaque jour par notre CERT concernant ces technologies vous seront envoyés et viendront enrichir vos plans d'action.

Mettre à jour

Réception des bulletins Yuno par email

Recevoir les bulletins de type PATCH EXPLOIT VULN

Recevoir les bulletins de criticité Aucune Faible Moyenne Élevée Critique

Yuno Rewind
Recevez par mail un condensé des derniers bulletins qui concernent votre périmètre et mettez à profit vos premiers tickets d'action.

Activer Yuno Rewind

Génération des tickets d'action

Langue des tickets d'action générés par Yuno Français Anglais

Ne pas générer de ticket d'action Générer des tickets d'action pour tous les bulletins du périmètre Générer des tickets d'action pour certains bulletins spécifiques (filtres indépendants des mails)

Notes

- Les paramètres d'envoi des bulletins Yuno par e-mail n'affectent pas la génération de tickets d'action.
- Le paramètre de langue ne concerne que les tickets d'action et non les e-mails envoyés.
- Attention, la modification de la langue de votre périmètre modifiera la langue des futurs tickets générés automatiquement par notre service Yuno.

Étape 2

Cliquez sur Préférences



Étape 3

Vous pouvez ici filtrer les bulletins techniques par criticité ou par type.

Ces filtres concerneront tous les utilisateurs du périmètre.

Étape 4

Vous pouvez ici choisir de générer des tickets d'action (selon le type ou la criticité des bulletins) afin d'alimenter le plan d'action associé à ce périmètre lors de la publication d'un bulletin de Veille.

Vous pouvez retrouver vos tickets d'action et suivre leur évolution dans le menu Plan d'Action, ou directement dans Mon plan d'action dans le menu latéral.

Exemple de configuration (1/2)

D'après mes préférences ci-contre, je vais recevoir **tous les bulletins de veille environnementale** de type **INFO** et **XMCO**, et disposant des criticités « **moyenne, élevée et alerte** ».

Pour les bulletins de type **INFO**, je ne recevrai que les bulletins disposant des tags **Finace** ou **Juridique**.

Veille technique

Réception de la veille technique

- Tout recevoir
- Appliquer les paramètres relatifs à mes périmètres

Veille informationnelle

Réception de la veille informationnelle :

- Tout recevoir
- Filtrée

Recevoir les bulletins de type :

INFO, XMCO

Recevoir les bulletins de criticité :

Moyenne, Élevée, Critique

Réception des bulletins de type INFO :

- Pas de filtrage par tag
- Filtrer sur les tags suivants:

Tags

x Finance x Règlementaire et Juridique

Reception des bulletins de type XMCO :

- Pas de filtrage par tag
- Filtrer sur les tags suivants:

x ▼ Tags ▼

D'après mes préférences, la réception de bulletins techniques suit les paramètres définis au sein de mes périmètres. C'est donc les périmètres auxquels je suis associé **qui vont déterminer la liste des bulletins techniques que je vais recevoir**.

Exemple de configuration (2/2)

Je fais partie du périmètre « base de données » qui recense 3 technologies (Elasticsearch, MongoDB et PostgreSQL).

Je recevrai donc **uniquement des bulletins techniques** faisant référence à ces 3 technologies.

 Plan d'actions  Technologie(s) déployée(s)

Technologies Déployées

Recherche _____

Elasticsearch

MongoDB

PostgreSQL

Périmètres > base de données

?

⚙

YU

 Plan d'actions  Technologie(s) déployée(s)  Composant(s) Technique(s)  Statistiques  Utilisateur(s)  Détails  Préférences

Cette page vous permet de gérer les options de réception des bulletins Yuno et de génération des tickets d'action associés aux technologies implémentées au sein de vos périmètres. Ces technologies peuvent être spécifiées lors de l'ajout d'un "Composant Technique" à votre périmètre d'audit.

Dès lors, les bulletins Yuno publiés chaque jour par notre CERT concernant ces technologies vous seront envoyés et viendront enrichir vos plans d'action.

Mettre à jour

Réception des bulletins Yuno par email

Recevoir les bulletins de type

PATCH
 EXPLOIT
 VULN

Recevoir les bulletins de criticité

Aucune
 Faible
 Moyenne
 Élevée
 Critique

Les préférences de mon périmètre « base de données » indiquent que je vais recevoir les bulletins techniques de type **PATCH** ou **VULN** et disposant des criticités **Élevée** ou **Alerte**.

Consulter le plan d'action

Le **plan d'action** vous permet d'accéder à l'ensemble des bulletins émis par le CERT-XMCO depuis le lancement du service de veille.

Yuno > Mon plan d'action

Intégrer les plans d'action de : Sélectionner un opérateur : égal à Tracker : Veille en vulnérabilité

Ajouter un filtre

Export PDF Référence Criticité Périmètre Titre Statut Impact Assigné à Publication

<input type="checkbox"/>	PDF 1458544		Global	[PATCH] [PERL] Prise de contrôle du système via deux vulnérabilités au sein de Perl	Nouveau	0	Alexandre PALLUT	01/12/2023
<input type="checkbox"/>	PDF 1458541		Global	[PATCH] [SOLARWINDS] Contournement de sécurité et manipulation de données via une vulnérabilité au sein de SolarWinds	Nouveau	0	Alexandre PALLUT	01/12/2023
<input type="checkbox"/>	PDF 1458537		Global	[PATCH] [APPLE] Prise de contrôle du système et divulgation d'informations via 2 vulnérabilités au sein de produits Apple (HT214032, HT214032, HT214033)	Nouveau	0	Alexandre PALLUT	01/12/2023
<input type="checkbox"/>	PDF 1458527		Global	[PATCH] [MICROSOFT] Contournement de sécurité via une vulnérabilité au sein de Microsoft Edge	Nouveau	0	Alexandre PALLUT	01/12/2023
<input type="checkbox"/>	PDF 1458519		Global	[PATCH] [GITLAB] Prise de contrôle du système et élévation de priviléges via 13 vulnérabilités au sein de GitLab	Nouveau	0	Alexandre PALLUT	01/12/2023
<input type="checkbox"/>	PDF 1458515		Global	[PATCH] [IBM] Manipulation de données et déni de service via 3 vulnérabilités au sein d'IBM Tivoli Netcool (7085933)	Nouveau	0	Alexandre PALLUT	01/12/2023
<input type="checkbox"/>	PDF 1458512		Global	[PATCH] [IBM] Prise de contrôle du système via une vulnérabilité au sein d'IBM AIX (7086090)	Nouveau	0	Alexandre PALLUT	01/12/2023
<input type="checkbox"/>	PDF 1458507		Global	[PATCH] [IBM] Déni de service via une vulnérabilité au sein d'IBM Tivoli Netcool/OMNibus_GUI (7085934)	Nouveau	0	Alexandre PALLUT	01/12/2023
<input type="checkbox"/>	PDF 1458502		Global	[PATCH] [REDHAT] Red Hat : 1 paquet mis à jour (postgresql)	Nouveau	0	Alexandre PALLUT	01/12/2023

Options d'affichage : Export XLS, Modifications multiples, AP

Cliquez sur le titre pour consulter l'action

Consulter la base XMCO

La **base XMCO** vous permet d'accéder à l'ensemble des bulletins émis par le CERT-XMCO depuis le lancement du service de veille.

Yuno

Mon plan d'action

Plan d'action

Base XMCO

Base CVE

Mes périmètres

Technologies

Statistiques

Yuno > Base XMCO

Recherche APT31

Éditeur

Produit

Criticité

Type

Filtres de recherche

Appliquer

Tags

DU

Au

Périmètres

Tous mes périmètres

Toutes les langues

Exclude les distributions Linux

Envoi par email

Export PDF

18/08/2023 [XMCO] Résumé de la semaine #33 (du 12 au 18 août) **Résumé de la semaine**

14/08/2023 [INFO] Campagne d'attaques d'APT31 ciblant des entreprises industrielles en Europe de l'Est **Europe de l'Est Services externes à distance**

21/07/2023 [INFO] Rapport sur les tactiques et techniques d'évasion des modes opératoires APT31 associés à la Chine **Compromission de chaîne d'approvisionnement Diplomatie Défense Suite d'informations Renseignement Télécommunications Amérique du Nord Europe de l'Ouest**

Cliquez sur le titre pour consulter le bulletin en ligne

Consulter la base CVE

La **base CVE** vous permet de rechercher les vulnérabilités associées à une version spécifique d'une technologie, ainsi que les bulletins XMCO ayant traité ces vulnérabilités.

Yuno

Mon plan d'action

Plan d'action

Base XMCO

Base CVE

Mes périmètres

Technologies

Statistiques

Filtres de recherche

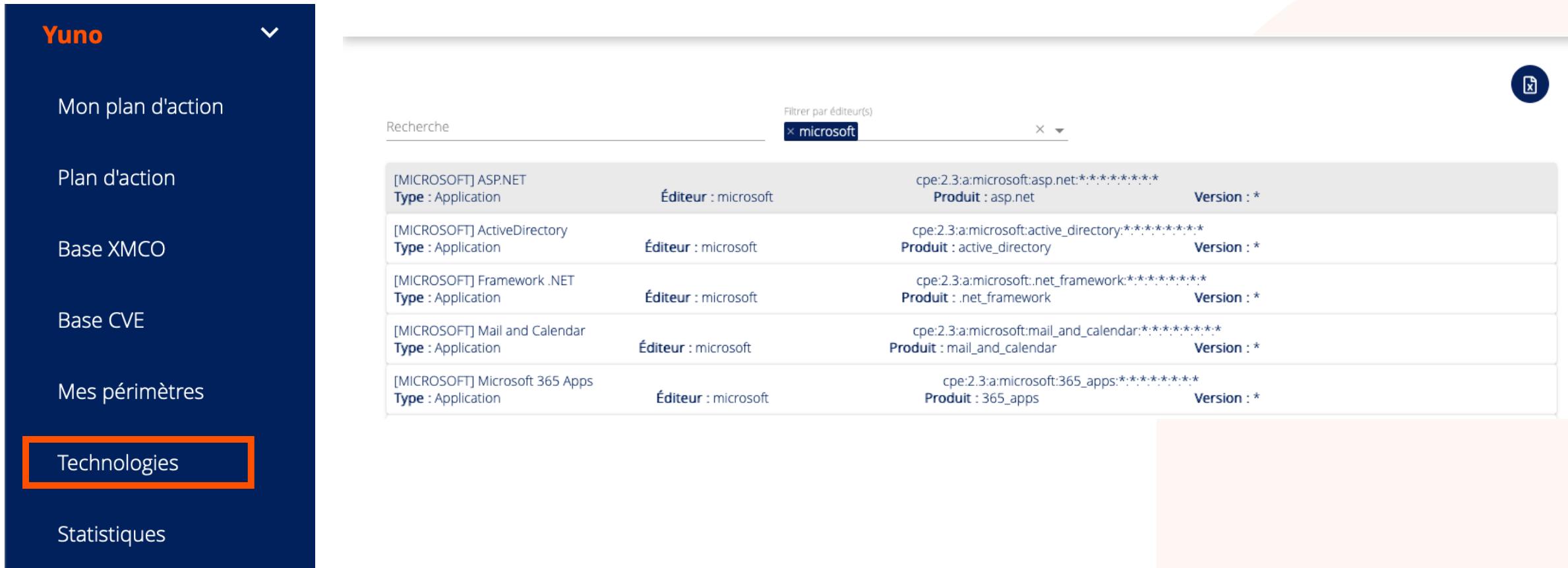
Éditeur	Produit	Version	Rechercher	C	≡	⚙		
Microsoft	Edge chromium	88.0.705.74						
CVE ID	Score CVSS (>=)	Du	Au					
Date de publication	CVE ID	CVSS	Éditeur	Produit	Version	Version mineure	CXA	Code d'exploitation
11/04/2023	CVE-2023-24935	0	Microsoft	Edge_chromium	88.0.705.74	*,*,*,*,*,*	CXA-2023-1848	
11/10/2022	CVE-2022-41035	5.3	Microsoft	Edge_chromium	88.0.705.74	*,*,*,*,*,*	CXA-2022-4762	, ... ⓘ
29/06/2022	CVE-2022-33638	8.3	Microsoft	Edge_chromium	88.0.705.74	*,*,*,*,*,*	CXA-2022-3078	
29/06/2022	CVE-2022-33639	8.3	Microsoft	Edge_chromium	88.0.705.74	*,*,*,*,*,*	CXA-2022-3078	
29/06/2022	CVE-2022-30192	8.3	Microsoft	Edge_chromium	88.0.705.74	*,*,*,*,*,*	CXA-2022-3078	
16/06/2022	CVE-2022-22021	5.1	Microsoft	Edge_chromium	88.0.705.74	*,*,*,*,*,*	CXA-2022-2800	, ... ⓘ

Les vulnérabilités CVE proviennent de la base officielle du MITRE

Bulletins XMCO faisant référence à la vulnérabilité

Technologies surveillées par le CERT-XMCO

La page des **technologies** vous permet de naviguer parmi l'ensemble des technologies et éditeurs suivis par le CERT-XMCO dans le cadre du service de veille.



The screenshot shows the Yuno web interface with a sidebar on the left and a main content area on the right.

Yuno (top left, in orange)

Mon plan d'action

Plan d'action

Base XMCO

Base CVE

Mes périmètres

Technologies (highlighted with an orange border)

Statistiques

Recherche (Search bar)

Filtrer par éditeur(s) (Filter by publisher(s))

microsoft (Selected filter)

Produit	Éditeur	CPE	Version
asp.net	microsoft	cpe:2.3:a:microsoft:asp.net:*	*
active_directory	microsoft	cpe:2.3:a:microsoft:active_directory:*	*
.net_framework	microsoft	cpe:2.3:a:microsoft:.net_framework:*	*
mail_and_calendar	microsoft	cpe:2.3:a:microsoft:mail_and_calendar:*	*
365_apps	microsoft	cpe:2.3:a:microsoft:365_apps:*	*

Consulter les statistiques

La page des **statistiques** vous permet d'obtenir des informations et KPI sur les bulletins reçus durant une période donnée

