Gestion des avis Cert/Aq

Réception des avis CertAq par courriel

Si CERTAQ-AVIS-XX-XXX - [SCADA] ; à ignorer pour l’instant.

Si CERTAQ-AVIS-XX-XXX ;

Faire une requête C2

 Faire une requête de service via les informations suivantes;

Site ; Hors site Incluant DMZ , local ; n/a , catalogue de service ; 436 SI , type de demande ; Avis de sécurité , Origine de la requête ; courriel , Supérieur ; Myriam Bourque

Inscrire les informations d’orientation

Ouvrir un bon de travail

 Si commutateur, Cisco, … => équipe Réseau

 Si applicatif => équipe SGAI Actif Clients

Exemple;

Date: 2022-11-10

Niveau de risque maximal= Important

Exploitation à distance = Oui

Exploitation locale= Oui

Exécution de code = Non

CVSS max 7.8

Produits vulnérables :

Apex One - versions 2019 (On-prem) sans le correctif de sécurité SP1 b11128

Apex One as a Service - versions sans le correctif de sécurité 220210 d'octobre 2022 (version de l'agent de sécurité : 14.0.11789)

 si oui ; procéder aux essais et au déploiement des mises à jour publiées par l'éditeur.

 si non ; fermer la requête.

Références :

Bulletin de sécurité Trend Micro du 9 novembre 2022:

https://success.trendmicro.com/dcx/s/solution/000291770?language=en\_US

Option de recherche du produit

Via le Microsoft Defender for Endpoint MDE

 Onglet gauche : Dans la section Points de terminaison, sélectionnez Gestion des Vulnérabilités, sélectionnez Stocks.

 Dans le menu Logiciel, il est possible d’effectuer la recherche.

 Des informations supplémentaires y sont disponible, tel les périphériques ayant le programme d’installer. L’exportation du dossier peut être fait et sera en Excel (.csv)

Via le SCCM accessible par le Citrix Workspace StoreFront

 Onglet en bas à gauche : Sélectionnez Surveillance

 Sélectionnez en double-cliquant le dossier Requêtes

 Sélectionnez en double-cliquant le dossier Soutien

 Sélectionnez en double-cliquant le dossier QR\_xxx désiré