BULLETIN DE VEILLE N°03

ANPT-2024-BV-03

« One of the main cyber-risks is to think they don't exist. The other is to try to treat all potential risks. »
- Stephane Nappo -

Mars 2024

Alertes de sécurité

Fortinet

Publication d'un exploit pour le bug RCE de Fortinet utilisé dans les attaques, correctif maintenant

21 Mars 2024

Des chercheurs en sécurité ont publié une démonstration de concept (PoC) pour exploiter une vulnérabilité critique dans le logiciel FortiClient Enterprise Management Server (EMS) de Fortinet, qui est maintenant activement exploitée dans des attaques.

Répertoriée sous le nom de CVE-2023-48788, cette faille de sécurité est une injection SQL dans le composant DB2 Administration Server (DAS), découverte et signalée par le National Cyber Security Centre (NCSC) du Royaume-Uni.

Elle concerne les versions 7.0 (7.0.1 à 7.0.10) et 7.2 (7.2.0 à 7.2.2) de FortiClient EMS et permet à des acteurs non authentifiés d'exécuter du code à distance avec des privilèges SYSTEM sur des serveurs non corrigés dans le cadre d'attaques peu complexes ne nécessitant pas d'interaction de la part de l'utilisateur.

"Une mauvaise neutralisation des éléments spéciaux utilisés dans une vulnérabilité de commande SQL ('SQL Injection') [CWE-89] dans FortiClientEMS peut permettre à un attaquant non authentifié d'exécuter du code ou des commandes non autorisés via des requêtes spécifiquement conçues," explique Fortinet dans un avis de sécurité publié la semaine dernière.

Jeudi, une semaine après que Fortinet a publié des mises à jour de sécurité pour corriger la faille de sécurité, les chercheurs en sécurité de l'équipe d'attaque d'Horizon3 ont publié une analyse technique et partagé un exploit de preuve de concept (PoC) qui aide à confirmer si un système est vulnérable sans fournir de capacités d'exécution de code à distance.

Shodan recense actuellement plus de 440 serveurs FortiClient Enterprise Management Server (EMS) exposés en ligne, tandis que le service de surveillance des menaces Shadowserver en a trouvé plus de 300, la plupart aux États-Unis.

En février, Fortinet a corrigé un autre bug RCE critique (CVE-2024-21762) dans le système d'exploitation FortiOS et le proxy web sécurisé FortiProxy, déclarant qu'il était "potentiellement exploité dans la nature".

Source : ***https://bit.ly/3vyBq23***

Kubernetes

La faille RCE de Kubernetes permet une prise de contrôle totale des nœuds Windows

13 Mars 2024

Un bug de sécurité dans le système de gestion de conteneurs Kubernetes largement utilisé permet aux attaquants d'exécuter du code à distance avec les privilèges System sur les terminaux Windows, ce qui peut potentiellement conduire à une prise de contrôle complète de tous les nœuds Windows au sein d'un cluster Kubernetes.

Tomer Peled, chercheur en sécurité chez Akamai, a découvert la faille, qui est répertoriée sous le nom de CVE-2023-5528 et a un score CVSS de 7,2. L'exploitation réside dans la manipulation des volumes Kubernetes, une fonctionnalité visant à prendre en charge le partage des données entre les pods sur un cluster, ou à les stocker de manière persistante en dehors du cycle de vie d'un pod. Comme vecteur d'attaque, les attaquants devraient créer des pods et des volumes persistants sur les nœuds Windows, ce qui leur permettrait d'escalader les privilèges d'administrateur sur ces nœuds, selon un listing GitHub pour la faille.

"Il est très facile d'exploiter cette vulnérabilité car un attaquant n'aurait qu'à modifier un paramètre et appliquer 3 fichiers YAML pour obtenir un RCE sur les points d'extrémité Windows", explique Peled à Dark Reading. Le cadre Kubernetes "utilise des fichiers YAML pour pratiquement tout", a-t-il écrit dans le billet. Les installations par défaut de Kubernetes antérieures à la version 1.28.4 fonctionnant à la fois sur des déploiements sur site et sur Azure Kubernetes Service sont vulnérables. L'équipe Kubernetes a été alertée de la faille et un correctif est disponible pour y remédier, ce qui est fortement recommandé.

Source : ***https://bit.ly/49dwaia***

Actualité

Des pirates informatiques affirment avoir pénétré dans le réseau informatique d'une installation israélienne

Un groupe de pirates informatiques lié à l'Iran affirme avoir pénétré dans le réseau informatique d'une installation nucléaire israélienne sensible, dans le cadre d'un incident déclaré par les pirates "Anonymous" comme une protestation contre la guerre à Gaza. Les pirates affirment avoir volé et publié des milliers de documents - notamment des fichiers PDF, des courriels et des diapositives PowerPoint - provenant du centre de recherche nucléaire Shimon Peres Negev. Cette installation secrète, qui abrite un réacteur nucléaire lié au programme d'armement nucléaire inavoué d'Israël, a toujours été la cible des roquettes du Hamas.

Dans un message sur les réseaux sociaux expliquant leurs intentions, le groupe a affirmé que "comme nous ne sommes pas aussi sanguinaires que Netanyahou et son armée terroriste, nous avons mené l'opération de manière à ce qu'aucun civil ne soit blessé".

Malgré cette déclaration, dans un autre message sur les réseaux sociaux, le groupe a indiqué qu'il n'avait "pas l'intention de provoquer une explosion nucléaire, mais que cette opération était dangereuse et que tout pouvait arriver", accompagné d'une vidéo d'animation représentant une détonation nucléaire et d'un appel à l'évacuation de la ville voisine de Dimona et de la localité de Yeruham.

Bien que les documents qui ont été publiés suggèrent que les pirates ont pu compromettre un réseau informatique connecté à l'installation, rien ne prouve qu'ils aient pu pénétrer dans son réseau de technologie opérationnelle (OT). Même si c'était le cas, les installations nucléaires disposent de nombreux systèmes de sécurité pour prévenir les incidents dangereux.

L'ambassade d'Israël à Londres n'a pas répondu à une demande de commentaire sur l'incident. Gil Messing, chef du personnel de la société israélienne de cybersécurité Checkpoint, a déclaré à Recorded Future News que sa société était au courant de l'existence du groupe Anonymous, qui a été créé avec ses propres comptes Twitter et Telegram vers le début de la guerre du pays contre le Hamas à Gaza.

Les cyberattaques contre Israël et ses alliés ont été "incessantes" depuis le début de la guerre, a-t-il déclaré. Les acteurs de la menace ont été à l'origine d'énormes décharges de données, se sont introduits dans des systèmes informatiques gouvernementaux, ont piraté des caméras de sécurité israéliennes, ont intensifié des campagnes de désinformation et ont pris pour cible des systèmes de contrôle industriel à l'autre bout du monde.

Dans le cas présent, Checkpoint a analysé les documents publiés par les pirates. "Nous pouvons dire qu'ils ne sont pas très sensibles pour la plupart (principalement autour des courriels, des noms, des fournisseurs avec lesquels ils travaillent), mais qu'ils pourraient l'être pour des attaques futures telles que le phishing et d'autres

Source: https://bit.ly/4axx6iA

L'Ukraine affirme avoir piraté les serveurs du ministère russe de la défense

La Direction principale du renseignement (GUR) du ministère ukrainien de la défense affirme avoir pénétré dans les serveurs du ministère russe de la défense (Minoborony) et volé des documents sensibles. Un communiqué de presse publié aujourd'hui sur un domaine officiel du gouvernement ukrainien décrit l'attaque comme une "opération spéciale" menée par les cyber-spécialistes du GUR.

À la suite de cette intrusion, le GUR affirme avoir obtenu des documents sensibles contenant des informations sur les services secrets, notamment des logiciels utilisé par le ministère russe de la défense pour protéger et crypter les données, Documents appartenant au vice-ministre russe de la défense, …etc.

Le communiqué de presse indique que le ministre en question, M. Ivanov, a joué un rôle important dans la réussite de la cyberattaque, bien que les détails de l'opération soient omis.

Quatre captures d'écran montrant des résultats d'interrogation de bases de données, des fichiers journaux et des documents décrivant les procédures/directives officielles ont été publiées comme preuves de l'infraction présumée.

BleepingComputer n'a pas été en mesure de valider l'authenticité de ces captures d'écran et a contacté le ministère russe de la Défense pour obtenir une déclaration, mais aucun commentaire n'était disponible dans l'immédiat.

Précédemment, le GUR a revendiqué des brèches non confirmées dans le Centre russe d'hydrométéorologie spatiale, alias "planeta" (планета), l'Agence fédérale russe du transport aérien, "Rosaviatsia", et le Service fédéral russe des impôts (FNS).

Deux de ces attaques auraient impliqué des sauvegardes de données et la destruction de bases de données dans le but de perturber les opérations. Dans la dernière affaire contre Moniborony, aucune revendication de ce type n'a été faite par le GUR.

Source : thttps://bit.ly/4arUdea

Bon à savoir

Pluie d'arnaques sur WhatsApp : voici comment les repérer pour mieux les contrer

Sur internet, aucun canal n'échappe aux hackers, pas même les messageries instantanées. Heureusement, quelques bonnes pratiques

limitent les risques. Il y a deux milliards d'utilisateurs actifs sur WhatsApp et sur Instagram. Autant dire tout le monde, au point d'avoir pris le pas sur les SMS. Bien ancrées dans notre quotidien, les messageries instantanées les plus populaires (WhatsApp, Messenger, Signal) sont devenues un terrain de jeu propice pour les hackers et les arnaqueurs.
Même si vous connaissez parfaitement l'émetteur, ne cliquez jamais sur les liens et les QR qu'il vous transmet. Vos contacts peuvent être de bonne foi et ne pas avoir conscience que certaines de ces URL correspondent à des sites frauduleux. C'est sans compter que, comme déjà évoqué, ils peuvent être sous le coup d'une arnaque, avec un hacker qui utilise son compte pour vous atteindre.
Dans le prolongement, faites preuve de méfiance et de retenue lorsque vos amis vous posent trop de questions via WhatsApp, que leur langage semble inhabituel ou hors de propos. En cas de doute sur son identité, contactez la personne par un autre canal pour vérifier s'il s'agit bien d'elle.
Enfin, pour garantir au mieux la confidentialité de ses données et éviter que des inconnus ne vous sollicitent intempestivement sur les messageries instantanées, il est essentiel de bien paramétrer l'application. Voici les principaux éléments à vérifier et à modifier :

- Optez pour un mot de passe robuste et, lorsque c'est possible, pour l'authentification à double facteurs (2FA) ;
- Désactivez la prévisualisation des images et des liens ;
- Ne laissez pas votre profil, votre statut et votre géolocalisation publique ;
- Bloquez tous les contacts qui ne seraient pas dans votre liste d'amis ;
- Maintenez à jour vos applications, ainsi que le système d'exploitation de votre smartphone, et limitez au strict minimum les autorisations qui leur sont accordées ;
- Vérifiez régulièrement les appareils connectés à vos messageries instantanées afin d'identifier au plus vite une compromission de votre compte. Lorsque c'est le cas, prévenez vos contacts sans attendre, que le piège ne se referme pas sur eux aussi.

Source : ***https://bit.ly/3TCULad***

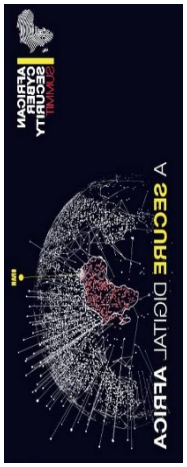
Evènements

Evènement a venir

African cyber security summit – La 6eme Edition

3-5 avril 2024 – Oran

https://acss.dz/



L'African Cyber Security Summit (ACSS) est le principal événement africain sur les questions de sécurité et de confiance numérique. Il réunit pendant 2 jours, les grands donneurs d'ordre de la Sécurité des Systèmes d'Information du continent, donnant une place unique à l'Algérie dans ce domaine. Plus de 300 participants représentant des institutions et des entreprises algériennes et africaines sont attendus au sixième Sommet prévu à Oran du 3 au 5 avril

Référence	ANPT-2024-BV-03
Titre	Bulletin de veille N°03
Date de version	31 Mars 2024
Contact	ssi@anpt.dz