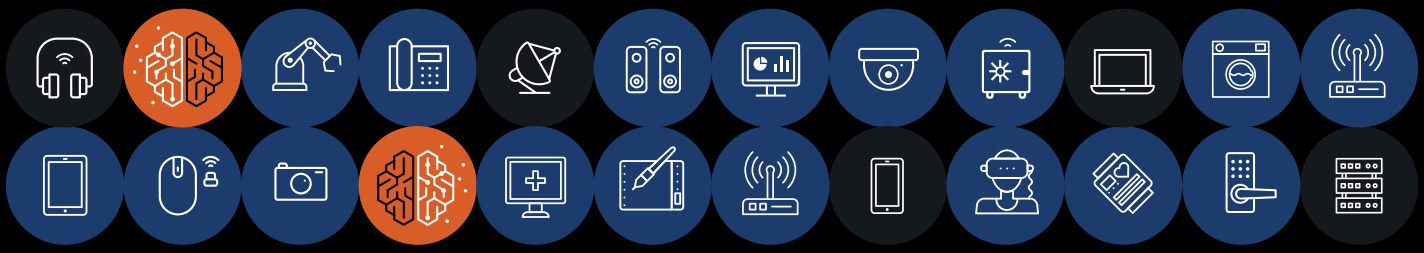
FORESCOUT
Active Defense for the Enterprise of Things™

AMNESIA:33

Synthèse du rapport de recherche



- Forescout Research Labs a lancé Project Memoria, **une initiative** visant à proposer à l'ensemble de la communauté de la cybersécurité **une étude de grande envergure sur la sécurité des piles TCP/IP**. L'objectif de Project Memoria est d'examiner de près les divers bugs courants à l'origine des vulnérabilités des piles TCP/IP, d'identifier les risques qu'elles représentent pour l'entreprise étendue et de définir les mesures permettant d'atténuer ces risques.
- **AMNESIA:33** est la première étude que nous publions dans le cadre de Project Memoria. Nous y évoquons les résultats de l'analyse de sécurité de sept **piles TCP/IP open source** et signalons une série de **33 nouvelles vulnérabilités** identifiées dans quatre des sept piles analysées, utilisées par d'importants fournisseurs d'appareils IoT, OT et IT.
- **Quatre des vulnérabilités dans AMNESIA:33 sont critiques** et peuvent potentiellement donner lieu à l'exécution de code à distance sur certains équipements. L'exploitation de ces vulnérabilités peut permettre à un cyberpirate de prendre le contrôle d'un appareil, pour ensuite l'employer comme point d'entrée à un réseau comportant des appareils connectés à Internet, comme point de départ de déplacements latéraux, comme point de persistance sur le réseau cible ou comme cible finale d'une attaque. Du point de vue des entreprises, ces vulnérabilités augmentent les risques de compromission de leur réseau ou de perturbation de leurs activités par des individus malveillants. Du point de vue des consommateurs, cela signifie que leurs appareils IoT peuvent être exploités à leur insu dans le cadre de campagnes d'attaque plus vastes (intégrés dans des réseaux d'ordinateurs zombies, par exemple).

> 150

FOURNISSEURS CONCERNÉS

forescout.com/amnesia33/ info-france@forescout.com Tél. (international) +1-408-213-3191

- Les vulnérabilités AMNESIA:33 concernent **plusieurs piles TCP/IP open source** qui appartiennent à **différents fournisseurs**. Cela signifie qu'une vulnérabilité tend à s'étendre **facilement et en toute discrétion** à plusieurs bases de code, équipes de développement, entreprises et produits, avec les défis importants que cela implique en matière de gestion des correctifs.
- Selon nos estimations, plus de 150 fournisseurs et des millions d'appareils sont vulnérables à AMNESIA:33. Cependant, il est **difficile d'estimer le véritable impact** d'AMNESIA:33, car les piles vulnérables sont très répandues (dans différents appareils IoT, OT et IT dans divers secteurs), hautement modulaires (avec des composants, fonctionnalités et paramètres présents en combinaisons diverses, et des bases de code empruntant différents parcours de développement) et incorporées dans des sous-systèmes fortement intégrés et non documentés. Pour ces mêmes raisons, ces vulnérabilités sont généralement très difficiles à éradiquer.
- Les piles TCP/IP affectées par AMNESIA:33 se trouvent dans des systèmes d'exploitation de matériel embarqué, des systèmes sur puce (SoC), des équipements réseau, des équipements OT et une myriade d'appareils IoT d'entreprise et grand public.
- Les piles TCP/IP constituent des composants critiques de tous les équipements connectés via le protocole IP, dont les appareils IoT/OT, puisqu'elles permettent une communication réseau de base. Une faille de sécurité dans une pile TCP/IP peut être extrêmement dangereuse, car le code de ces composants peut être utilisé pour **traiter *tous* les paquets réseau entrant sur un appareil**. Cela signifie que certaines vulnérabilités affectant une pile TCP/IP permettent d'exploiter un appareil même lorsqu'il est simplement connecté à un réseau, sans exécuter aucune application particulière.
- Un grand nombre des vulnérabilités signalées dans le cadre de l'étude **AMNESIA:33** sont le fait de pratiques de développement logiciel contestables, comme l'absence de validation d'entrée de base. Elles sont principalement liées à la **corruption de la mémoire** et peuvent provoquer des **dénis de service, des fuites d'informations** ou l'**exécution de code à distance**.
- L'identification et la correction des appareils vulnérables constituent des tâches extrêmement complexes ; dès lors, la gestion des vulnérabilités des piles TCP/IP devient un énorme défi pour la communauté de la cybersécurité. Nous recommandons d'**adopter des solutions qui offrent une visibilité granulaire sur les appareils**, permettent la surveillance des communications réseau et isolent les appareils ou segments réseau vulnérables afin de gérer au mieux le risque que posent ces vulnérabilités.

Détecter, c'est bien. Sécuriser, c'est mieux.

Contactez-nous dès aujourd'hui pour protéger activement votre Enterprise of Things.

Télécharger le rapport complet (en anglais) : Prenez connaissance des résultats complets de notre étude et des mesures d'atténuation des risques qui peuvent être mises en place.

Télécharger le livre blanc (en anglais) : Découvrez comment Forescout vous aide à protéger activement votre entreprise des vulnérabilités AMNESIA:33, notamment grâce à six bonnes pratiques.

Regarder le webinar (en anglais) : Écoutez nos experts expliquer les grandes lignes de notre étude.

forescout.com/amnesia33/ info-france@forescout.com Tél. (international) +1-408-213-3191

FORESCOUT
Active Defense for the Enterprise of Things™

Forescout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 (États-Unis)

Email info-france@forescout.com
Tél. (international) +1-408-213-3191
Support +1-708-237-6591

Pour en savoir plus, consultez le site Forescout.fr