**CYBER DEFENSE AFRICA** : ANNONCE DE SÉCURITÉ **Date** : 30/12/2024

| Type de Contenu | Description |
|---|---|
| Titre | ***Vulnérabilité des routeurs Four-Faith en cours d'exploitation (CVE-2024-12856)*** |
| ID | *202412/AS/98* |
| Code TLP | *Green* |
| Niveau de risque | ***Critique*** |
| Application et service affectés | *Firmware des Routeurs Four-Faith avec des fonctions de gestion à distance* |
| Version / Edition | *Modèles concernés :*<br>• ***F3x24 :*** *Inclut les sous-modèles comme F3424, F3524, et F3624.*<br>• ***F3x36 :*** *Inclut les sous-modèles comme F3436, F3536, et F3636.* |
| Plateforme | ***Four-Faith*** |
| Mise à jour | *Vulnérabilité corrigée dans les versions récentes* |
| Résumé | ***Une importante vulnérabilité post-authentification affectant les routeurs industriels Four-Faith est activement exploitée*** |
| Impacts | - ***Injection de commandes OS***<br>- ***Accès à distance non autorisé***<br>- ***Exécution des shells inversés sur le***<br>- ***Vol et exfiltration d'informations sensibles et confidentielles.*** |
| Description Détaillée | *Une nouvelle vulnérabilité post-authentification affectant les routeurs industriels Four-Faith est exploitée dans des attaques.*<br>*Identifiée sous* ***CVE-2024-12856****, cette vulnérabilité permet aux attaquants d'utiliser les informations d'identification par défaut du routeur pour injecter des commandes à distance non authentifiées :*<br>*L'attaque peut être menée au moins contre les routeurs Four-Faith F3x24 et F3x36 via HTTP en utilisant* ***/apply.cgi****.*<br>*Ces modèles de routeurs sont vulnérables à l'injection de commande OS dans leur paramètre* ***adj_time_year*** *lors de la modification de l'heure système de l'appareil via* ***submit_type=adjust_sys_time.*** |
| Recommandations | - *Modifier les informations d'identification par défaut en les remplaçant par des identifiants sécurisés.*<br>- *Consulter les sources officielles de Four-Faith pour connaître et appliquer les mises à jour des firmwares disponibles ou les correctifs ciblant CVE-2024-12856.*<br>- *Déployer la règle « Suricata » fournie pour surveiller le trafic réseau et détecter les tentatives d'exploitation en cours.* |

| | |
|---|---|
| | - *Isoler les systèmes de contrôle industriel (ICS/SCADA) des réseaux externes pour réduire les vecteurs d'attaque.* |
| Indicateurs de Compromission | ***Adresses IP :*** *178.215.238.91* |
| Liens pour plus de détails | - *https://www.fourfaith.com/industrial-5g-router/*<br>- *https://vulncheck.com/blog/four-faith-cve-2024-12856* |

```
alert http any any -> any any ( \
    msg:"VULNCHECK Four-Faith CVE-2024-12856 Exploit Attempt"; \
    flow:to_server; \
    http.method; content:"POST"; \
    http.uri; content:"/apply.cgi"; startswith; \
    http.header_names; content:"Authorization"; \
    http.request_body; content:"change_action="; \
    content:"adjust_sys_time"; \
    pcre:"/adj_time_[^=]+=[a-zA-Z0-9]*[^a-zA-Z0-9=]/"; \
    classtype:web-application-attack; \
    reference:cve,CVE-2024-12856; \
    sid:12700438; rev:1;)
```

*Figure 1: Script de la règle « suricata » pour détecter l'exploitation en cours de la CVE-2024-12856*