Patch Infrastructure

Sécuriser les serveurs en patchant OpenSSH et OpenSSL

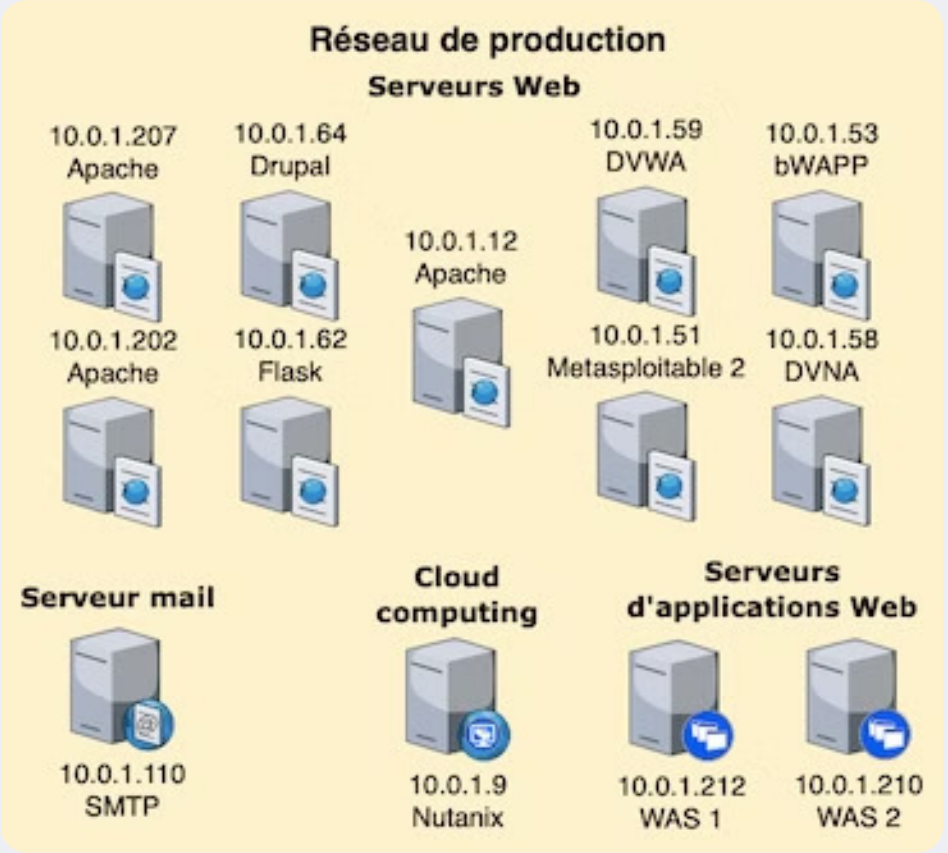
Présentation des machines vulnérables

Machines :

- **10.0.1.53 :** serveur web avec bWAPP et Ubuntu 14.04
- **10.0.1.210 :** serveur d'application web et Ubuntu 22.04

Importance : Les deux serveurs jouent un rôle crucial dans l'infrastructure

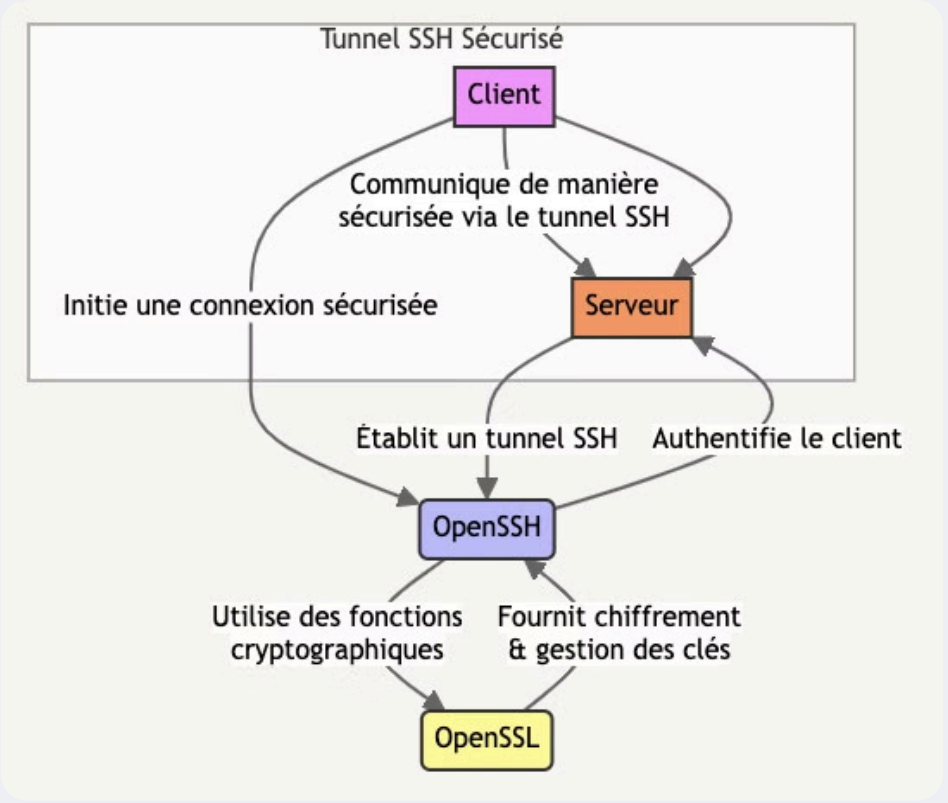
Objectif : sécuriser ces serveurs en patchant OpenSSH et OpenSSL



Présentation de la vulnérabilité

OpenSSH : Protocole pour sécuriser les communications entre un client et un serveur via SSH.

OpenSSL : Bibliothèque permettant des communications sécurisées via SSL/TLS, utilisée par de nombreux logiciels, y compris OpenSSH.

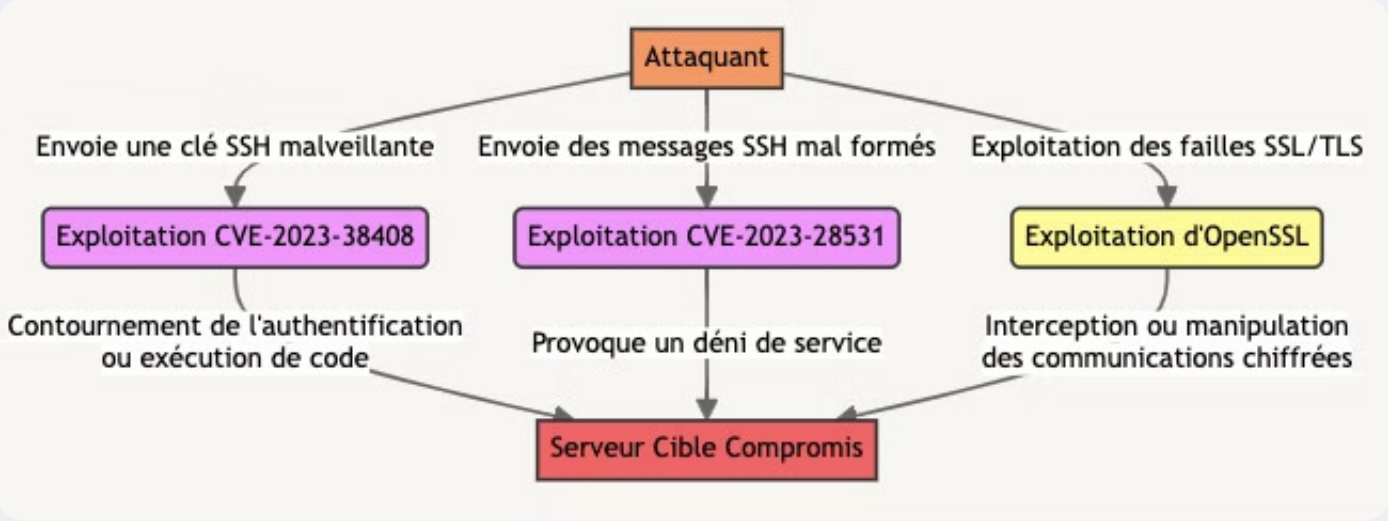


Détail des vulnérabilités

La **CVE-2023-38408 (OpenSSH)** permet l'exécution de code arbitraire en exploitant un défaut dans la gestion des clés SSH.

La **CVE-2023-28531 (OpenSSH)** permet un déni de service par l'exploitation de messages SSH mal formés.

Impact sur OpenSSL : Risque de compromission des communications chiffrées si une faille similaire existe dans les versions non mises à jour.



Préparation pour le patch

Vérification des **versions obsolètes** d'OpenSSH et OpenSSL

Identification des **dépendances** entre les deux logiciels.

```
root@ip-10-0-1-53:~# sudo apt upgrade openssh-server
Reading package lists ... Done
Building dependency tree
Reading state information ... Done
Calculating upgrade ... Done
openssh-server is already the newest version.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.

125 additional updates are available with UA Infrastructure ESM.
To see these additional updates run: apt list --upgradable
See https://ubuntu.com/advantage or run: sudo ua status
root@ip-10-0-1-53:~# ssh -V
OpenSSH_6.6.1p1 Ubuntu-2ubuntu2.13, OpenSSL 1.0.1f 6 Jan 2014
```

```
7f7173033125:~# cd openssh-9.3p1/
7f7173033125:~/openssh-9.3p1# apk add build-base openssl openssl-dev zlib-dev
```

Téléchargement et préparation des sources

Téléchargement des dernières versions sources d'OpenSSH et OpenSSL pour Ubuntu 14.04 (machine 10.0.1.53) et Ubuntu 22.04 (machine 10.0.1.210).

Préparation des fichiers pour la compilation.

```
root@ip-10-0-1-53:~# wget https://cdn.openbsd.org/pub/OpenBSD/OpenSSH/portable/openssh-9.3p2.tar.gz
--2024-07-01 15:04:28--  https://cdn.openbsd.org/pub/OpenBSD/OpenSSH/portable/openssh-9.3p2.tar.gz
```

```
7f7173033125:/usr/local/openssl$ wget https://www.openssl.org/source/openssl-3.0.14.tar.gz
```

```
7f7173033125:/usr/local/openssl$ wget https://cdn.openbsd.org/pub/OpenBSD/OpenSSH/portable/openssh-9.3p1.tar.gz
```

```
7f7173033125:/# export LD_LIBRARY_PATH=/usr/local/lib:$LD_LIBRARY_PATH
7f7173033125:/# export PKG_CONFIG_PATH=/usr/local/lib/pkgconfig:$PKG_CONFIG_PATH
7f7173033125:/# export LDFLAGS="-L/usr/local/lib"
7f7173033125:/# export CPPFLAGS="-I/usr/local/include"
```

Compilation d'OpenSSL et OpenSSH

Préparation de l'environnement : Configuration des chemins pour les bibliothèques nécessaires.

Téléchargement des sources : Obtention des fichiers source et installation des dépendances.

Configuration et compilation : Exécution des commandes pour compiler et installer OpenSSL et OpenSSH.

Vérification finale : Confirmation de la présence des bibliothèques critiques après l'installation.

```
root@ip-10-0-1-53:~/openssh-9.3p2# make
root@ip-10-0-1-53:~/openssh-9.3p2# sudo make install
```

```
root@ip-10-0-1-53:~# tar -xzf openssh-9.3p2.tar.gz
root@ip-10-0-1-53:~# cd openssh-9.3p2
root@ip-10-0-1-53:~/openssh-9.3p2# ./configure
```

```
7f7173033125:~# cd openssh-9.3p1/
7f7173033125:~/openssh-9.3p1# ./configure --with-ssl-dir=/usr/local --prefix=/usr/local --with-ldflags="-L/usr/local/lib" --wi
th-cppflags="-I/usr/local/include"
```

```
7f7173033125:~/openssh-9.3p1# make
```

```
7f7173033125:~/openssh-9.3p1# make install
```

```
7f7173033125:/# cd root
7f7173033125:~# ls
openssh-9.3p1          openssh-9.3p1.tar.gz   openssl-3.0.14         openssl-3.0.14.tar.gz
7f7173033125:~# ls -al
total 16820
drwx------    1 root     root          4096 Jul  2 14:21 .
drwxr-xr-x    1 root     root          4096 Jul  2 12:06 ..
-rw-------    1 root     root         16315 Jul  2 14:42 .ash_history
-rw-------    1 root     root          1090 Jul  1 15:18 .bash_history
-rw-r--r--    1 root     root            41 Jul  2 13:58 .profile
drwxr-xr-x    2 root     root          4096 Jun 30 20:49 .ssh
-rw-r--r--    1 root     root           205 Jul  2 13:34 .wget-hsts
drwxr-xr-x    7 git      git          12288 Jul  2 14:39 openssh-9.3p1
-rw-r--r--    1 root     root       1856839 Mar 15  2023 openssh-9.3p1.tar.gz
drwxrwxr-x   21 root     root          4096 Jul  2 13:55 openssl-3.0.14
-rw-r--r--    1 root     root      15305497 Jun  4 15:04 openssl-3.0.14.tar.gz
7f7173033125:~# vi /.profile
```

Validation du patch

Vérification des versions mises à jour d'OpenSSH et OpenSSL.

Tests de connectivité pour s'assurer du bon fonctionnement des services.

```
root@ip-10-0-1-53:~/openssh-9.3p2# sudo service ssh restart
```

```
root@ip-10-0-1-53:~/openssh-9.3p2# ssh -V
OpenSSH_9.3p2, OpenSSL 1.0.1f 6 Jan 2014
```

```
7f7173033125:~/openssh-9.3p1# /usr/local/bin/ssh -V
OpenSSH_9.3p1, OpenSSL 1.0.2t  10 Sep 2019
```

```
7f7173033125:~/openssl-3.0.14# openssl version
OpenSSL 3.0.14 4 Jun 2024 (Library: OpenSSL 3.0.14 4 Jun 2024)
```

Explication des dépendances

Qu'est-ce qu'une dépendance ? : Une dépendance est un logiciel ou une bibliothèque dont un autre programme a besoin pour fonctionner.

Dépendances résolues :

- OpenSSH dépend d'OpenSSL pour le chiffrement.
- Résolution des dépendances liées aux bibliothèques `libssl.so.3` et `libcrypto.so.3`.

```
7f7173033125:~/openssh-9.3p1# ls /usr/local/lib/libssl.so.3
/usr/local/lib/libssl.so.3
7f7173033125:~/openssh-9.3p1# ls /usr/local/lib/libcrypto.so.3
/usr/local/lib/libcrypto.so.3
```

Comparaison Avant/Après

Machine	*Composant*	*Version Avant Mise à Jour*	*Version Après Mise à Jour*
10.0.1.210	**OpenSSH**	7.5p1	9.3p1
10.0.1.210	**OpenSSL**	1.1.1	3.0.14
10.0.1.53	**OpenSSH**	6.6.1p1	9.3p1
10.0.1.53	**OpenSSL**	1.0.1	3.0.14

Bénéfices du patch

Aspect	Avant	Après
Sécurité	Vulnérable aux exploits connus	Sécurisé contre les exploits connus
Performance	Risque de lenteurs dues à des versions non optimisées	Amélioration de la performance grâce aux optimisations des nouvelles versions
Compatibilité	Obsolète, support limité, difficulté à intégrer les nouvelles technologies	Compatible avec les technologies modernes et les futures mises à jour

Recommandations pour l'avenir

1

Mise à jour régulière :

Planifiez des mises à jour régulières pour éviter que les logiciels ne deviennent obsolètes et vulnérables.

2

Automatisation des Mises à Jour :

Utiliser des outils d'automatisation pour réduire le risque d'erreur humaine et garantir une mise à jour continue.

3

Monitoring :

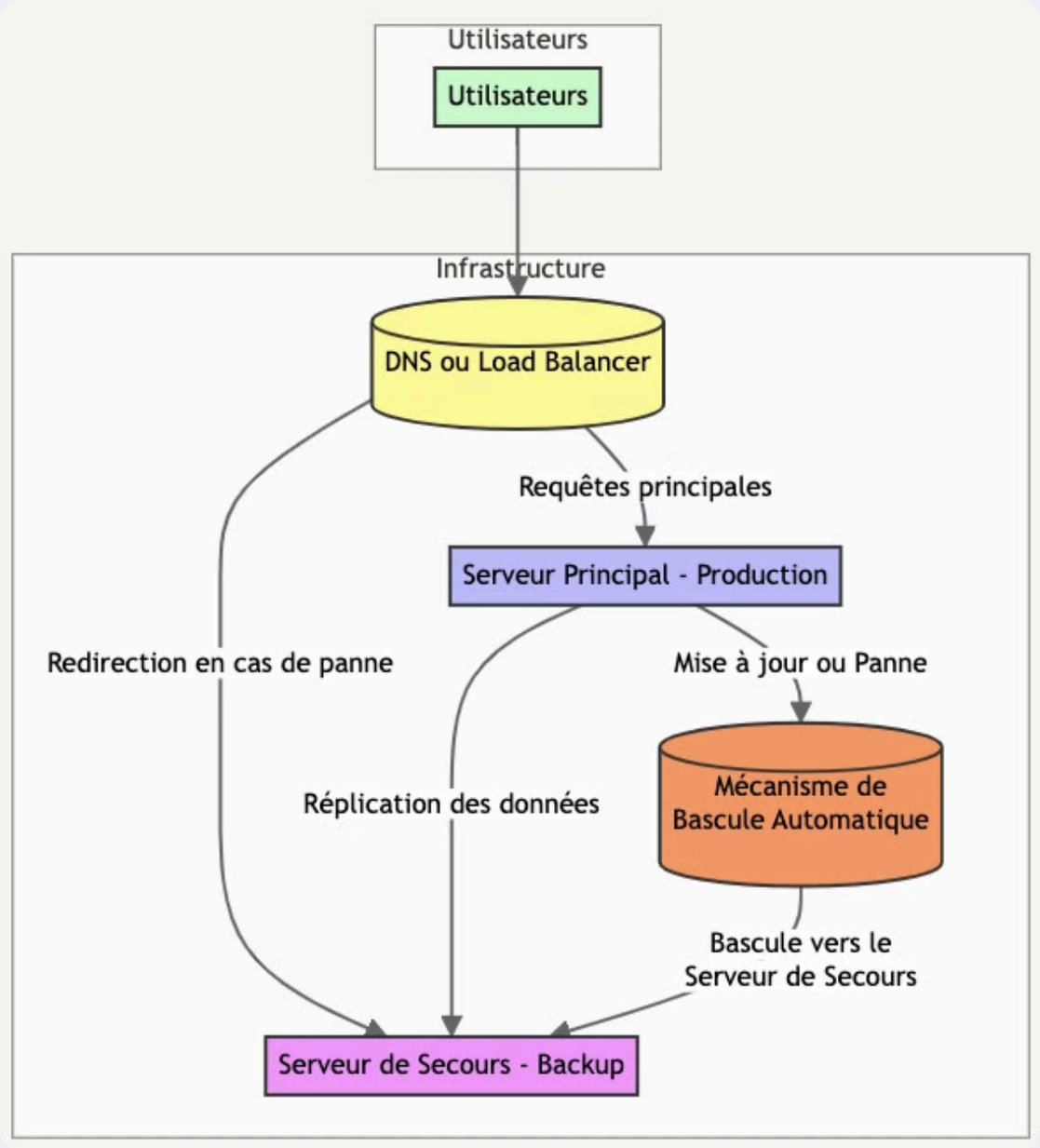
Mettre en place une surveillance active pour détecter les vulnérabilités dès qu'elles apparaissent.

4

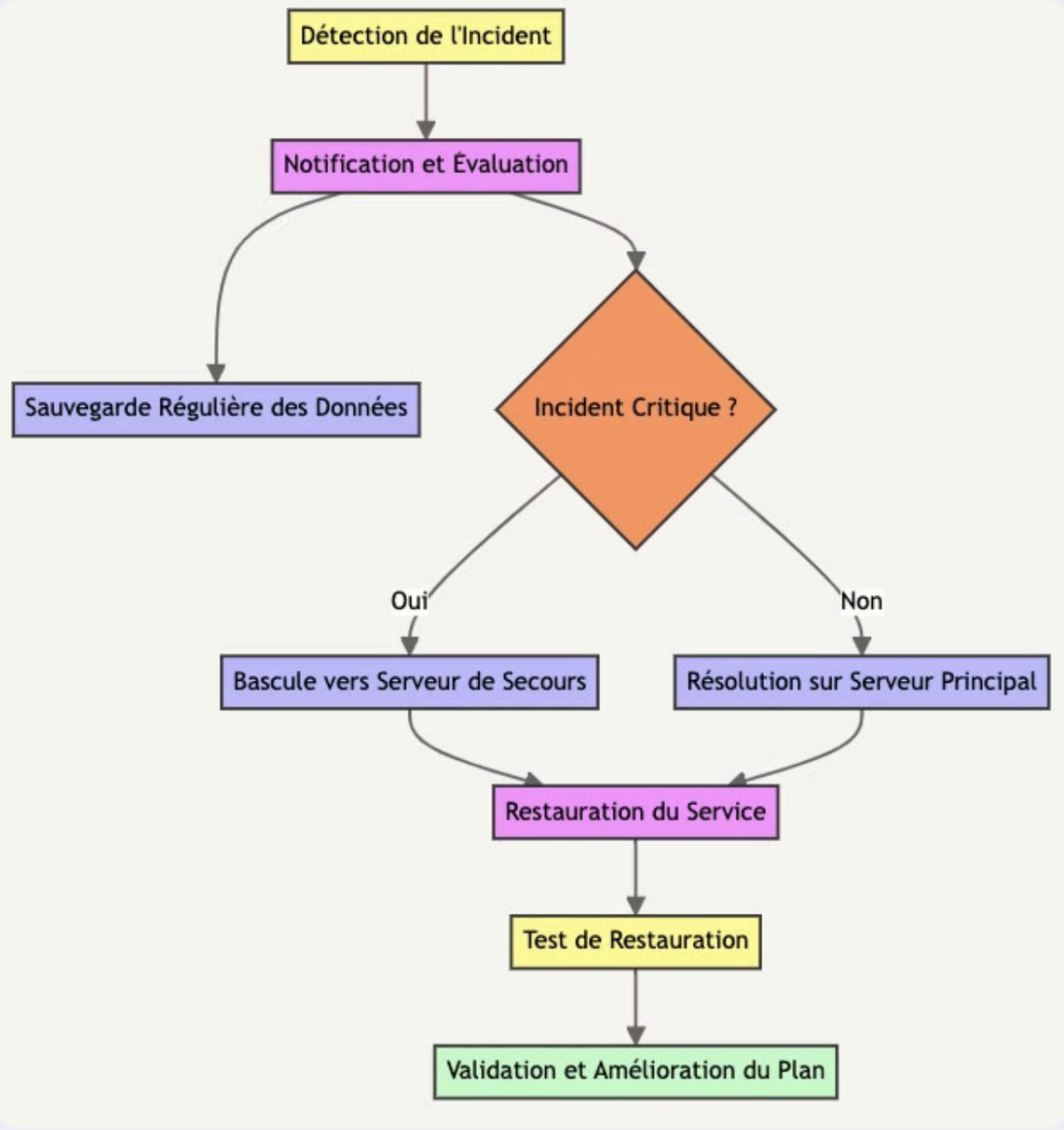
Impact Économique :

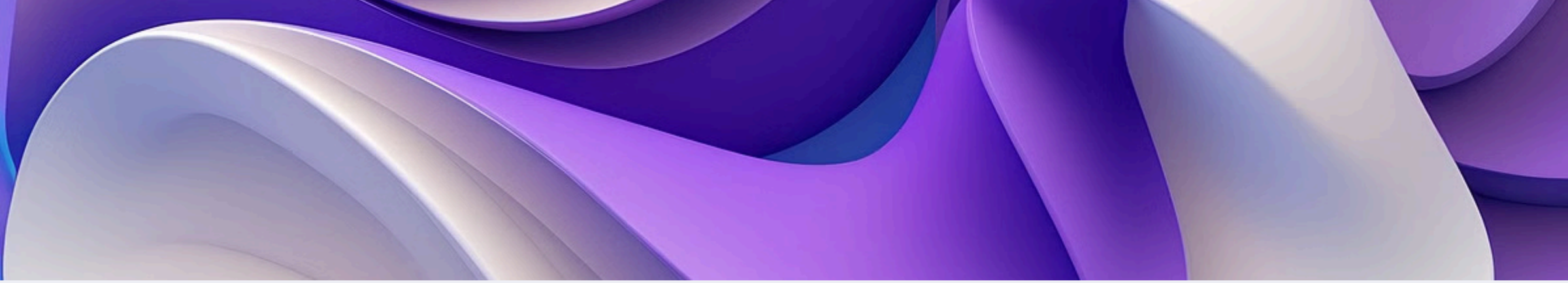
Réduction des coûts liés aux interruptions imprévues grâce à une maintenance proactive.

Gestion de l'Interruption d'activité



Recommandations pour la continuité d'activité





Synthèse

- **Renforcement de la Sécurité** : Les mises à jour d'OpenSSH et OpenSSL ont corrigé des vulnérabilités critiques, renforçant ainsi la sécurité des serveurs 10.0.1.53 et 10.0.1.210.
- **Amélioration de la Performance et de la Compatibilité** : Les serveurs sont désormais optimisés et compatibles avec les technologies modernes, ce qui garantit leur performance et leur fiabilité.
- **Plan de Continuité** : L'infrastructure est maintenant mieux préparée à gérer les interruptions et à assurer une continuité de service grâce à des solutions redondantes et des procédures de sauvegarde et de restauration.
- **Impact Économique** : La mise en œuvre de ces améliorations permet de réduire les coûts opérationnels à long terme en minimisant les interruptions et en assurant une maintenance proactive.

Merci pour votre attention

Avez vous des questions ?