



**RÉPUBLIQUE
FRANÇAISE**

*Liberté
Égalité
Fraternité*



25 avril 2024

Note de recommandations techniques réactives pour la mise en sécurité des ouvrages hydrauliques

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) a été informée de plusieurs incidents chez des exploitants de barrages (équipés de vannes motorisées) et de centrales hydroélectriques liés à des attaques informatiques. Ces actes malveillants d'origine cyber ont consisté en la modification des paramétrages ou le déclenchement d'actions à distance telles que l'ouverture de vannes au niveau d'un barrage, une perte temporaire de production électrique ou la destruction d'un automate.

Les attaquants semblent principalement tirer parti d'une faiblesse dans la sécurisation du serveur d'accès à distance (tels que VNC, Teamviewer, Anydesk, Logmein, etc.) utilisé pour le pilotage des organes de commandes des installations. Ils tirent notamment parti de l'existence de comptes et de mots de passe triviaux sur ces serveurs. L'exposition directe, sur Internet, d'autres interfaces de gestion serait également utilisée par les attaquants.

L'ANSSI vous recommande par conséquent d'agir ou de faire modifier vos installations par votre installateur, en appliquant les mesures de sécurité élémentaires suivantes pour les connexions d'accès à distance :

- Limiter les adresses IP sources autorisées à se connecter vers l'installation au niveau du routeur, ou de la box ADSL, que ce soit pour un usage du bureau à distance ou pour des protocoles industriels vers un automate ;
- Utiliser autant que possible un VPN pour se connecter à l'installation : la plupart des box-ADSL, grand public ou professionnelles, permettent aujourd'hui d'installer un VPN pour l'accès à distance. Dans la plupart des cas, aucun équipement additionnel n'est requis ;
- Vérifier les comptes existants et changer l'ensemble des mots de passe (accès au terminal IHM de maintenance, accès VNC, accès aux automates, etc.) pour des mots de passe complexes et robustes¹ et activer dans la mesure du possible les options d'authentification à multiples facteurs si elles sont disponibles² ;
- Reparamétrer le client et le serveur d'accès distance pour utiliser un protocole sécurisé tel qu'un accès VPN TLS1.3 ou IPSEC, ou le protocole SSH pour VNC ;
- Toujours utiliser un logiciel d'accès distant maintenu à jour par son éditeur ;

¹ <https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/mots-de-passe>

² <https://cyber.gouv.fr/publications/recommandations-relatives-lauthentification-multifacteur-et-aux-mots-de-passe>



**RÉPUBLIQUE
FRANÇAISE**

*Liberté
Égalité
Fraternité*



- Toujours utiliser la version la plus récente du logiciel d'accès distant (client et serveur) en effectuant des mises à jour régulières afin de bénéficier des correctifs de sécurité publiés par l'éditeur ;
- Dans la mesure du possible, utiliser des postes dédiés et séparer les flux pour l'administration de vos équipements³.

Si ces actions ne sont pas réalisables pour des raisons économiques ou techniques, il est vivement recommandé de déconnecter les installations d'Internet et d'en réaliser la gestion sur place.

En cas de suspicion de compromission, vous trouverez des conseils ainsi que des contacts sur la page dédiée à ce sujet du site du CERT-FR⁴.

³ <https://cyber.gouv.fr/publications/la-cybersecurite-des-systemes-industriels>

⁴ <https://www.cert.ssi.gouv.fr/les-bons-reflexes-en-cas-dintrusion-sur-un-systeme-dinformation>