ZyXEL introduit une faille dans ses pare-feu

Prière de mettre à jour le *firmware* de nos *firewalls* physiques. C'est, dans les grandes lignes, le message que fait passer ZyXEL.

L'équipementier taïwanais avait publié le *firmware* en question le 10 novembre 2020. Dix-neuf jours plus tard, un chercheur lui avait signalé la présence d'une faille. Cette vulnérabilité repose sur un compte administrateur non documenté. ZyXEL dit l'avoir implémenté pour faciliter la mise à jour automatique de ses pare-feu par FTP.

Les identifiants du compte sont codés en dur. Problème : il est possible d'y accéder en clair… et on ne peut les modifier.
L'ensemble est utilisable aussi bien en SSH que sur la console web. Avec, entre autres conséquences, de potentielles modifications des règles de pare-feu, l'interception de trafic et la création de comptes VPN pour accéder au réseau en aval.

La faille touche aussi les contrôleurs Wi-Fi NXC2500 et NXC5500 en versions 6.00 à 6.10. Le tableau ci-dessous résume la situation.

Affected product series	Patch available in
Firewalls	
ATP series running firmware ZLD V4.60	ZLD V4.60 Patch1 in Dec. 2020
USG series running firmware ZLD V4.60	ZLD V4.60 Patch1 in Dec. 2020
USG FLEX series running firmware ZLD V4.60	ZLD V4.60 Patch1 in Dec. 2020
VPN series running firmware ZLD V4.60	ZLD V4.60 Patch1 in Dec. 2020
AP controllers	
NXC2500 running firmware V6.00 through V6.10	V6.10 Patch1 on Jan. 8, 2021
NXC5500 running firmware V6.00 through V6.10	V6.10 Patch1 on Jan. 8, 2021

Sur ces *firewalls*, les VPN SSL utilisent le port 443. La console web, qui exploite le même port, se retrouve ainsi souvent exposée au réseau internet. Plus de 100 000 appareils seraient dans ce cas, affirme le chercheur à l'origine de la découverte.
Interroger ces équipements en tant qu'utilisateur non authentifié ne permet pas d'obtenir directement la version de *firmware* installée. On peut toutefois la déterminer en fonction de certains fichiers CSS et JavaScript qui remontent.

Des tests réalisés aux Pays-Bas sur un échantillon de 1000 appareils donnent un taux de vulnérabilité de 10 %. La proportion aurait pu être plus importante si les mises à jour automatiques n'étaient pas désactivées par défaut.

ZyXEL avait publié un premier patch le 8 décembre 2020. Une semaine plus tard, tous les appareils touchés avaient leur correctif.

*Photo d'illustration (*firewall *VPN300) © Zyxel*