SEQURETEK

BACKDOOR ACCOUNT IN ZYXEL DEVICES

OVERVIEW

Zyxel devices contain a hardcoded administrative backdoor account in firmware version 4.60, that can grant attackers admin level access to devices via either the SSH interface or the web administration panel.

KNOWLEDGE BASE REGISTER

- Version Control

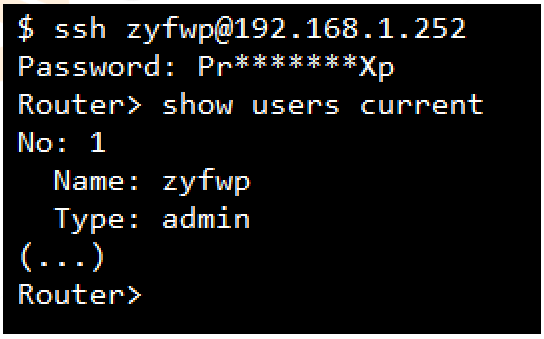
Issue Date	Version	Prepared by	Approved by
5th Jan 2021	v 1.0	Vidhi Patel	Cdr. Subhash Dutta

OVERVIEW

- Zyxel has **released a patch for the hardcoded credential vulnerability, tracked as CVE-2020-29583 in multiple devices firmware version 4.60.**
- Affected devices contains an **undocumented account (zyfwp) with an unchangeable password in firmware.**
- Zyxel devices including **Unified Security Gateway (USG), Advanced Threat Protection (ATP), Unified Security Gateway (USG) FLEX** and **VPN firewalls**, products are affected from this flaw.
- Globally, more than 1,00,000 devices have exposed their web interface to the internet and vulnerable with this critical flaw.
- Successful exploitation could completely compromise the confidentiality, integrity and availability of the device.

TECHNICAL DETAILS

- Researcher from EYE Netherlands discovered an uncovered admin account name "**zyfwp**" with the default password "**PrOw!****Xp**" stored in plaintext in Firmware.
- The account has admin level access, Because It is **used to install firmware updates to other interconnected Zyxel devices via FTP**.



```
$ ssh zyfwp@192.168.1.252
Password: Pr*******Xp
Router> show users current
No: 1
  Name: zyfwp
  Type: admin
(...)
Router>
```

Figure 1: Backdoor Account

- With hardcoded credentials user can **login to the SSH server or web interface with admin privileges.** The user "zyfwp" is not visible in the interface and its password cannot be changed.
- By exploiting this vulnerability attackers **can change firewall settings to allow or block certain traffic.** They could also **intercept traffic or create VPN accounts to gain access to the network behind the device.** Combined with a vulnerability like Zerologon this could be devastating to small and medium businesses.

- State-sponsored hacking groups and ransomware groups could abuse this backdoor account to access vulnerable devices for additional attacks in network.

AFFECTED PRODUCTS

Affected product series	Patch available in
Firewalls	
ATP (Advanced Threat Protection) series running firmware ZLD V4.60	ZLD V4.60 Patch1 in Dec. 2020
USG (Unified Security Gateway) 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	V6.10 Patch1 on Jan. 8, 2021
NXC5500	V6.10 Patch1 on Jan. 8, 2021

PREVENTIVE AND CORRECTIVE DEFENCE ACTIONS

- Update to the latest firmware version.
- Enhance account security by Two-Factor Authentication.
- Change the default password as soon as you log in to a new device for the first time.
- Use strong, unique passwords for every device and change them regularly.
- Don't enable remote access unless it's absolutely necessary.