Hackers start exploiting the new backdoor in Zyxel devices

bleepingcomputer.com/news/security/hackers-start-exploiting-the-new-backdoor-in-zyxel-devices/

Lawrence Abrams

By
Lawrence Abrams

- January 6, 2021
- 03:00 AM
- 0

Threat actors are actively scanning the Internet for open SSH devices and trying to login to them using a new recently patched Zyxel hardcoded credential backdoor.

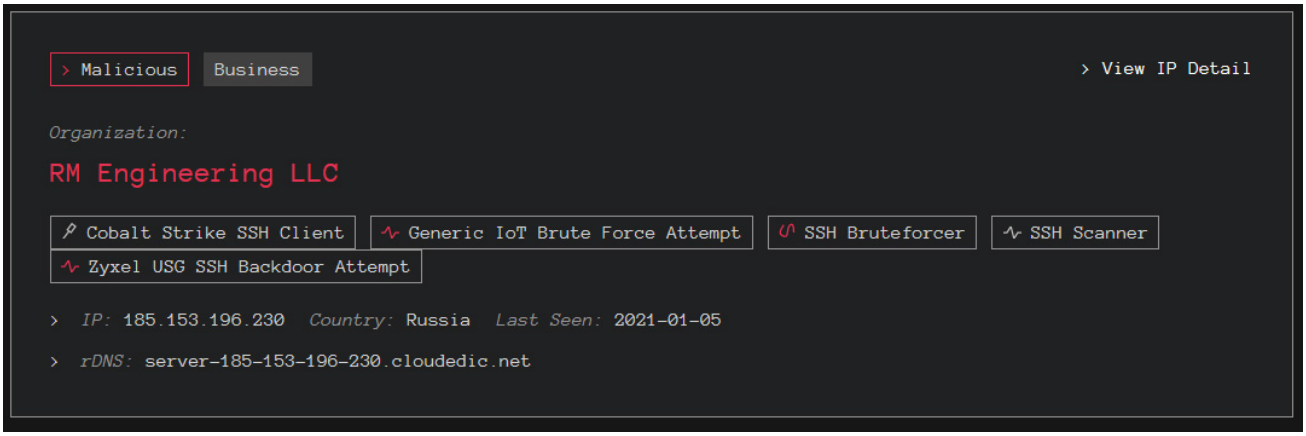
Last month, Niels Teusink of Dutch cybersecurity firm EYE disclosed a secret hardcoded backdoor account in Zyxel firewalls and AP controllers. This secret 'zyfwp' account allowed users to login via SSH and the web interface to gain administrator privileges.

In an advisory, Zyxel states that they used the secret account to deliver firmware updates via FTP automatically.

This backdoor is a significant risk as it could allow threat actors to create VPN accounts to gain access to internal networks or port forward Internal services to make them remotely accessible and exploitable.

Threat actors actively scan for Zyxel backdoor

Yesterday, cybersecurity intelligence firm GreyNoise detected three different IP addresses actively scanning for SSH devices and attempting to login to them using the Zyxel backdoor credentials.



IP address scanning for Zyxel SSH backdoor

GreyNoise CEO Andrew Morris told BleepingComputer that the threat actor does not appear to be scanning specifically for Zyxel devices but is instead scanning the Internet for IP addresses running SSH.

When SSH is detected, it will attempt to brute force an account on the device, with one of the credentials tested being the new Zyxel 'zyfwp' backdoor account.

Of particular interest is that one of the IP addresses is using the built-in SSH client of Cobalt Strike to perform the scans. Morris told BleepingComputer that the actor might be scanning this way to evade threat intelligence vendors.

> Since May of this year, GreyNoise has observed an unknown actor quietly fingerprinting SSH honeypots on the Internet, exclusively through Tor. The actor is using Cobalt Strike's SSH client. This is likely being done to avoid threat intelligence vendors.https://t.co/UUN9VCuyfG pic.twitter.com/vGxInpR84M
>
> — GreyNoise (@GreyNoiseIO) September 16, 2020

Zyxel released the 'ZLD V4.60 Patch 1' last month that removes the backdoor accounts on firewall devices. Zyxel announced yesterday that they would release the patch for AP controllers on January 8th, 2021.

BleepingComputer strongly recommends that all users install the patch as soon as possible to prevent threat actors from gaining access to vulnerable networks, deploying ransomware, or stealing data.

Related Articles:

Hackers are exploiting critical bug in Zyxel firewalls and VPNs

Zyxel patches critical bug affecting firewall and VPN devices

Zyxel warns of flaws impacting firewalls, APs, and controllers

BPFDoor: Stealthy Linux malware bypasses firewalls for remote access

Protect your devices anywhere with this portable VPN, Firewall deal

- Backdoor
- Firewall
- SSH
- VPN
- Zyxel

Lawrence Abrams

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.

- Previous Article
- Next Article

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: