Backdoor account discovered in more than 100,000 Zyxel firewalls, VPN gateways

zdnet.com/article/backdoor-account-discovered-in-more-than-100000-zyxel-firewalls-vpn-gateways

By Catalin Cimpanu for Zero Day | January 2, 2021 -- 03:59 GMT (19:59 PST) | Topic: Security

Image: Zyxel

More than 100,000 Zyxel firewalls, VPN gateways, and access point controllers contain a hardcoded admin-level backdoor account that can grant attackers root access to devices via either the SSH interface or the web administration panel.

Also: Best VPNs

Device owners are advised to update systems as soon as time permits.

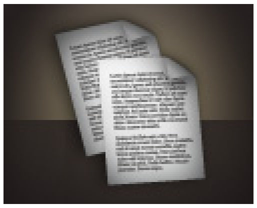
Security experts warn that anyone ranging from DDoS botnet operators to state-sponsored hacking groups and ransomware gangs could abuse this backdoor account to access vulnerable devices and pivot to internal networks for additional attacks.

Affected modules include many enterprise-grade devices

Affected models include many of Zyxel's top products from its line of business-grade devices, usually deployed across private enterprise and government networks.

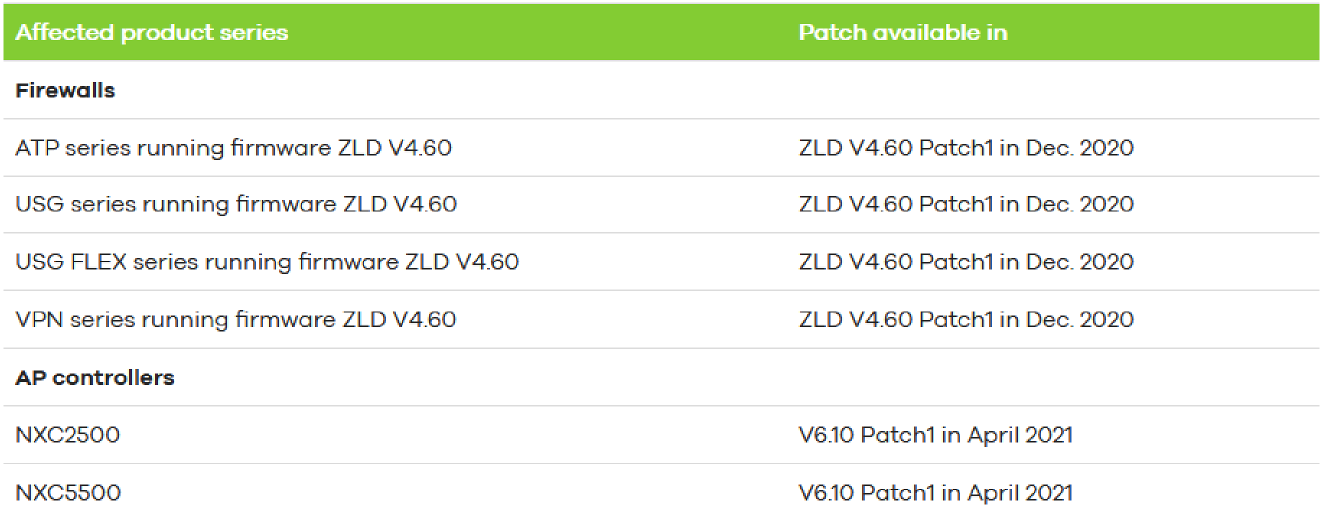
This includes Zyxel product lines such as:

- the Advanced Threat Protection (ATP) series - used primarily as a firewall
- the Unified Security Gateway (USG) series - used as a hybrid firewall and VPN gateway
- the USG FLEX series - used as a hybrid firewall and VPN gateway
- the VPN series - used as a VPN gateway
- the NXC series - used as a WLAN access point controller



Many of these devices are used at the edge of a company's network and, once compromised, allow attackers to pivot and launch further attacks against internal hosts.

Patches are currently available only for the ATP, USG, USG Flex, and VPN series. Patches for the NXC series are expected in April 2021, according to a Zyxel security advisory.



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	V6.10 Patch1 in April 2021
NXC5500	V6.10 Patch1 in April 2021

Backdoor account was easy to discover

Installing patches removes the backdoor account, which, according to Eye Control researchers, uses the "**zyfwp**" username and the "**PrOw!aN_fXp**" password.

"The plaintext password was visible in one of the binaries on the system," the Dutch researchers said in a report published before the Christmas 2020 holiday.

Researchers said the account had root access to the device because it was being used to install firmware updates to other interconnected Zyxel devices via FTP.

Zyxel should have learned from the 2016 backdoor incident

In an interview with *ZDNet* this week, IoT security researcher Ankit Anubhav said that Zyxel should have learned its lesson from a previous incident that took place in 2016.

Tracked as CVE-2016-10401, Zyxel devices released at the time contained a secret backdoor mechanism that allowed anyone to elevate any account on a Zyxel device to root level using the "**zyad5001**" SU (super-user) password.

"It was surprising to see yet another hardcoded credential specially since Zyxel is well aware that the last time this happened, it was abused by several botnets," Anubhav told *ZDNet*.

"CVE-2016-10401 is still in the arsenal of most password attack based IoT botnets," the researcher said.

But this time around, things are worse with CVE-2020-29583, the CVE identifier for the 2020 backdoor account.

Anubhav told *ZDNet* that while the 2016 backdoor mechanism required that attackers first have access to a low-privileged account on a Zyxel device — so they can elevate it to root —, the 2020 backdoor is worse as it can grant attackers direct access to the device without any special conditions.

"In addition, unlike the previous exploit, which was used in Telnet only, this needs even lesser expertise as one can directly try the credentials on the panel hosted on port 443," Anubhav said.

Furthermore, Anubhav also points out that most of the affected systems are also very varied, compared to the 2016 backdoor issue, which only impacted home routers.

Attackers now have access to a wider spectrum of victims, most of which are corporate targets, as the vulnerable devices are primarily marketed to companies as a way to control who can access intranets and internal networks from remote locations.

A new wave of ransomware and espionage?

This is a big deal in the bigger picture because vulnerabilities in firewalls and VPN gateways have been one of the primary sources of ransomware attacks and cyber-espionage operations in 2019 and 2020.

Security flaws in Pulse Secure, Fortinet, Citrix, MobileIron, and Cisco devices have often been exploited to attack companies and government networks.

The new Zyxel backdoor could expose a whole new set of companies and government agencies to the same type of attacks that we've seen over the past two years.

By Catalin Cimpanu for Zero Day | January 2, 2021 -- 03:59 GMT (19:59 PST) | Topic: Security