The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
01/04/2021

SUBJECT:
A vulnerability in Zyxel Firewall and AP Controllers Could Allow for Administrative Access

OVERVIEW:
A vulnerability has been discovered in Zyxel Firewall and AP Controllers, which could allow for remote administrative access. Zyxel is a manufacturer of networking devices that provides networking equipment globally. Successful exploitation of this vulnerability could allow for administrative access to the system, which could allow an attacker to change firewall settings, intercept traffic, create VPN accounts to gain access to the network behind the device, and perform additional administrative functions.

THREAT INTELLIGENCE:
There are currently no reports of this vulnerability being exploited in the wild.

SYSTEMS AFFECTED:
- Zyxel Firewall ATP, USG, USG FLEX, and VPN version 4.60
- Zyxel AP Controllers NXC2500 and NXC5500 version 6.10

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY:
A Vulnerability has been discovered in Zyxel Firewall and AP Controllers, which could allow for remote administrative access. This vulnerability exists due to hardcoded credentials being used to update firewall and AP controllers firmware. The accounts login name is ‘zyfwp’ and has a static plain-text password which cannot be changed and has administrative privileges. This could allow an attacker to use this users account to login remotely and could potentially result in a compromise of the Zyxel device. This could allow the attacker to change firewall settings,

intercept traffic, create VPN accounts to gain access to the network behind the device, and other administrative functions.

RECOMMENDATIONS:
The following actions should be taken:

- Apply appropriate updates provided by Zyxel to vulnerable systems, immediately after appropriate testing.
- Run all software as a non-privilege user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.
- Apply the Principle of Least Privilege to all systems and services.

REFERENCES:
Zyxel:
https://www.zyxel.com/support/CVE-2020-29583.shtml

BleepingComputer:
https://www-bleepingcomputer-com.cdn.ampproject.org/c/s/www.bleepingcomputer.com/news/security/secret-backdoor-discovered-in-zyxel-firewall-and-ap-controllers/amp/

EYE:
https://www.eyecontrol.nl/blog/undocumented-user-account-in-zyxel-products.html

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-29583