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
www.cisa.gov/tlp
Information may be distributed without restriction, subject to standard copyright rules.

DATE(S) ISSUED:
03/29/2022

SUBJECT:
A Vulnerability in Zyxel Firewall Could Allow for Authentication Bypass

OVERVIEW:
A vulnerability has been discovered in versions of Zyxel Firewall's CGI program which could allow for authentication bypass. Zyxel Firewall is a next generation firewall product which enables users to manage, detect and respond to threats on the network. Successful exploitation of this vulnerability could allow an attacker to bypass authentication and obtain administrative access to the device. Malicious actors with administrative access may be able to view, change, or delete sensitive data.

THREAT INTELLIGENCE:
There is currently no reports of this vulnerability being publicly exploited.

SYSTEMS AFFECTED:

- USG/ZyWALL - ZLD V4.20 through ZLD V4.70
- USG FLEX - ZLD V4.50 through ZLD V5.20
- ATP - ZLD V4.32 through ZLD V5.20
- VPN - ZLD V4.30 through ZLD V5.20
- NSG V1.20 through V1.33 Patch 4

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**

- Small business entities: **High**

Home users: Low

TECHNICAL SUMMARY:
A vulnerability has been discovered in versions of Zyxel Firewall's CGI program which could allow for authentication bypass. Zyxel Firewall is a next generation firewall product which enables users to manage, detect and respond to threats on the network. Successful exploitation of this vulnerability could allow an attacker to bypass authentication and obtain administrative access to the device. Malicious actors with administrative access may be able to view, change, or delete sensitive data.

RECOMMENDATIONS:

We recommend the following actions be taken:

- Apply updates provided by Zyxel to vulnerable systems immediately after appropriate testing.
- 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/Zyxel-security-advisory-for-authentication-bypass-vulnerability-of-firewalls.shtml

CVE:
https://www.cve.org/CVERecord?id=CVE-2022-0342