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:
05/16/2022

SUBJECT:
A vulnerability in Zyxel Firewall and VPN Could Allow for Arbitrary Code Execution

OVERVIEW:
A vulnerability has been discovered in Zyxel Firewall and VPN, which could allow for arbitrary code execution. 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:
A proof-of-concept writeup was posted to Rapid7 on May 12, 2022. There has been reports of this vulnerability being exploited in the wild.

SYSTEMS AFFECTED:

- USG FLEX 100(W), 200, 500, 700 ZLD V5.00 through ZLD V5.21 Patch 1
- USG FLEX 50(W) / USG20(W)-VPN ZLD V5.10 through ZLD V5.21 Patch 1
- ATP series ZLD V5.10 through ZLD V5.21 Patch 1
- VPN series ZLD V4.60 through ZLD V5.21 Patch 1

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 Zyxel Firewall and VPN, which could allow for arbitrary code execution. This vulnerability exists in the CGI program of some firewall versions which could allow an attacker to modify specific files and then execute some OS commands on a vulnerable device. The accounts login name executing commands is “nobody”. Successful exploitation of this vulnerability could allow for arbitrary code execution in the context of the nobody user. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

Tactic: Initial Access (TA0001)

Technique: Exploit Public-Facing Application (T1190)

RECOMMENDATIONS:

We recommend the following actions be taken:

- Apply appropriate updates provided by Zyxel to vulnerable systems, immediately after appropriate testing. (M1051: Update Software)
    - **Safeguard 7.1: Establish and Maintain a Vulnerability Management Process**: Establish and maintain a documented vulnerability management process for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.
    - **Safeguard 7.4: Perform Automated Application Patch Management:** Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.
    - **Safeguard 7.5: Perform Automated Vulnerability Scans of Internal Enterprise Assets:** Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.
- Run all software as a non-privilege user (one without administrative privileges) to diminish the effects of a successful attack. (M1026: Privileged Account Management)
    - **Safeguard 4.7: Manage Default Accounts on Enterprise Assets and Software:** Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.
    - **Safeguard 5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts:** Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user’s primary, non-privileged account.

- Apply the Principle of Least Privilege to all systems and services. (M1042: Disable or Remove Feature or Program)
    - **Safeguard 16.10: Apply Secure Design Principles in Application Architectures:** Apply secure design principles in application architectures. Secure design principles include the concept of least privilege and enforcing mediation to validate every operation that the user makes, promoting the concept of "never trust user input." Examples include ensuring that explicit error checking is performed and documented for all input, including for size, data type, and acceptable ranges or formats. Secure design also means minimizing the application infrastructure attack surface, such as turning off unprotected ports and services, removing unnecessary programs and files, and renaming or removing default accounts.

REFERENCES:

CVE:https://www.cve.org/CVERecord?id=CVE-2022-30525

Zyxel:https://www.zyxel.com/us/en/support/Zyxel-security-advisory-for-OS-command-injection-vulnerability-of-firewalls.shtml

Rapid7:https://www.rapid7.com/blog/post/2022/05/12/cve-2022-30525-fixed-zyxel-firewall-unauthenticated-remote-command-injection/

BleepingComputer:https://www.bleepingcomputer.com/news/security/hackers-are-exploiting-critical-bug-in-zyxel-firewalls-and-vpns/