مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Exploited Vulnerability in Zyxel Firewalls

Tracking #:432316589

Date:04-12-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Zyxel has identified an active threat targeting Zyxel firewalls, exploiting previously disclosed vulnerabilities.

TECHNICAL DETAILS:

Zyxel has identified an active threat targeting Zyxel firewalls, exploiting previously disclosed vulnerabilities. Specifically, CVE-2024-11667, a directory traversal vulnerability in the web management interface, has been used by threat actors to potentially gain unauthorized access to devices.

Vulnerabilities Details:

- CVE Identifier: CVE-2024-11667
- Vulnerability Type: Directory Traversal
- Affected Devices: Zyxel ZLD firewalls running firmware versions 5.00 through 5.38.
- Vulnerability Description: A directory traversal vulnerability exists in the web management interface of Zyxel ZLD firewall firmware versions 5.00 through 5.38.
  This flaw allows attackers to upload or download files by manipulating a specially crafted URL, potentially compromising the device's file system and enabling unauthorized access or code execution.
- Severity: Critical (As per recent exploitation attempts, this vulnerability is actively targeted by threat actors, posing a significant risk to affected systems).
- Exploited Versions: Versions 5.00 to 5.38.
- Fixed Version: Firmware version 5.39, released on September 3, 2024. This update resolves CVE-2024-11667 and includes further security enhancements

RECOMMENDATIONS:

- Users with affected devices should immediately update their Zyxel firewall to fixed firmware version.
- If it is not possible to update firmware immediately, temporarily disable remote access to your device. This will limit external exposure and help mitigate the risk of an attack until the necessary updates can be applied.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-protecting-against-recent-firewall-threats-11-27-2024