مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

Critical Vulnerabilities in Zyxel Routers

Tracking #:432316833

Date:06-02-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed critical vulnerabilities in several Zyxel router models that could be exploited to gain complete control of affected devices.

TECHNICAL DETAILS:

Critical vulnerabilities CVE-2025-0890 and CVE-2024-40891 exists in multiple Zyxel Customer Premises Equipment (CPE) devices, allowing unauthenticated attackers to execute arbitrary code and gain full control over affected routers. These vulnerabilities are actively being exploited in the wild.

Vulnerabilities Details:

- **CVE-2024-40891**:
  - CVSS Base Score: 9.8 Critical
  - Authenticated command injection vulnerability in the Telnet service.
- **CVE-2025-0890**:
  - CVSS Base Score: 8.8 High
  - Presence of default credentials, including "supervisor:zyad1234" and "zyuser:1234".
- These vulnerabilities can be chained together, allowing unauthenticated code execution via Telnet.
- Successful exploitation of this vulnerability could allow attackers to:
  - Execute arbitrary code on affected devices
  - Gain full control over routers
  - Steal data
  - Launch further attacks
  - Disrupt internet connectivity

Affected Devices:
The following Zyxel router models are likely vulnerable:

- VMG1312-B10A, VMG1312-B10B, VMG1312-B10E
- VMG3312-B10A, VMG3313-B10A, VMG3926-B10B
- VMG4325-B10A, VMG4380-B10A
- VMG8324-B10A, VMG8924-B10A
- SBG3300, SBG3500

RECOMMENDATIONS:

- **Replace Vulnerable Devices:** Zyxel has confirmed that the affected models are end-of-life and recommends upgrading to newer, supported devices.
- **Disable Telnet Access:** Since Telnet is an insecure protocol, users should disable it immediately to prevent unauthorized access.
- **Change Default Credentials:** Ensure that default credentials are not in use. Create strong, unique passwords for all user accounts.
- **Monitor Network Traffic:** Keep an eye on unusual network activity that may indicate exploitation attempts.

- **Segment Network Devices:** Isolate potentially vulnerable routers from critical network infrastructure to limit potential damage.

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://nvd.nist.gov/vuln/detail/CVE-2025-0890
- https://nvd.nist.gov/vuln/detail/CVE-2024-40891
- https://vulncheck.com/blog/zyxel-telnet-vulns