مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates- Multiple Vulnerabilities Zyxel NAS devices

Tracking #:432315924

Date:05-06-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council observed that Zyxel Networks released an emergency security update to address multiple vulnerabilities affecting older NAS devices that have reached end-of-life.

TECHNICAL DETAILS:

Zyxel has released security patches to address three critical vulnerabilities (CVE-2024-29972, CVE-2024-29973, CVE-2024-29974) impacting older NAS devices (NAS326 and NAS542) that have reached end-of-life (EOL). These vulnerabilities allow unauthenticated attackers to remotely execute malicious code and compromise affected devices.

Vulnerabilities Details

- **CVE-2024-29972 (Critical):** Command injection vulnerability in a CGI program allowing remote attackers to execute arbitrary commands with root privileges.
- **CVE-2024-29973 (Critical):** Command injection vulnerability in a specific parameter allowing remote attackers to execute arbitrary commands.
- **CVE-2024-29974 (Critical):** Remote code execution vulnerability in a CGI program allowing attackers to upload malicious configuration files.
- Two additional vulnerabilities (CVE-2024-29975 and CVE-2024-29976) were identified but not fixed due to the EOL status of the devices. These vulnerabilities allow privilege escalation and information disclosure to authenticated attackers.
- Proof-of-concept (PoC) exploit code is publicly available.

Affected Versions:

- Zyxel NAS326 devices running firmware versions 5.21(AAZF.16)C0 and earlier
- Zyxel NAS542 devices running firmware versions 5.21(ABAG.13)C0 and earlier

Fixed Versions:

- NAS326: Update to firmware version 5.21(AAZF.17)C0 or later.
- NAS542: Update to firmware version 5.21(ABAG.14)C0 or later.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released by Zyxel.

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://outpost24.com/blog/zyxel-nas-critical-vulnerabilities/
- https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-nas-products-06-04-2024