مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

# Critical Vulnerability in Zyxel Products

Tracking #:432316213

Date:03-09-2024

## EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Zyxel has released a security advisory addressing a critical vulnerability in its Access Point (AP) and Router versions.

## TECHNICAL DETAILS:

**Vulnerability Details**:

- **CVE-2024-7261 |** Base Score: 9.8 | Severity: Critical | COMMAND INJECTION
  - The identified resides in the improper neutralization of special elements within the "host" parameter of the CGI program used in certain Zyxel access points (APs) and security routers. Exploiting this vulnerability, an attacker could send a specially crafted cookie to the vulnerable device, thereby executing OS commands without authentication.
  - This type of exploit opens the door to significant risks, including data breaches, network compromise, and disruption of services.

**Affected Versions and Respective Fixes**:

| Product | Affected model | Affected version | Patch availability |
|---|---|---|---|
| AP | NWA50AX | 7.00(ABYW.1) and earlier | 7.00(ABYW.2) |
| | NWA50AX PRO | 7.00(ACGE.1) and earlier | 7.00(ACGE.2) |
| | NWA55AXE | 7.00(ABZL.1) and earlier | 7.00(ABZL.2) |
| | NWA90AX | 7.00(ACCV.1) and earlier | 7.00(ACCV.2) |
| | NWA90AX PRO | 7.00(ACGF.1) and earlier | 7.00(ACGF.2) |
| | NWA110AX | 7.00(ABTG.1) and earlier | 7.00(ABTG.2) |
| | NWA130BE | 7.00(ACIL.1) and earlier | 7.00(ACIL.2) |
| | NWA210AX | 7.00(ABTD.1) and earlier | 7.00(ABTD.2) |
| | NWA220AX-6E | 7.00(ACCO.1) and earlier | 7.00(ACCO.2) |
| | NWA1123-AC PRO | 6.28(ABHD.0) and earlier | 6.28(ABHD.3) |
| | NWA1123ACv3 | 6.70(ABVT.4) and earlier | 6.70(ABVT.5) |
| | WAC500 | 6.70(ABVS.4) and earlier | 6.70(ABVS.5) |
| | WAC500H | 6.70(ABWA.4) and earlier | 6.70(ABWA.5) |
| | WAC6103D-I | 6.28(AAXH.0) and earlier | 6.28(AAXH.3) |
| | WAC6502D-S | 6.28(AASE.0) and earlier | 6.28(AASE.3) |
| | WAC6503D-S | 6.28(AASF.0) and earlier | 6.28(AASF.3) |
| | WAC6552D-S | 6.28(ABIO.0) and earlier | 6.28(ABIO.3) |
| | WAC6553D-E | 6.28(AASG.2) and earlier | 6.28(AASG.3) |
| | WAX300H | 7.00(ACHF.1) and earlier | 7.00(ACHF.2) |
| | WAX510D | 7.00(ABTF.1) and earlier | 7.00(ABTF.2) |
| | WAX610D | 7.00(ABTE.1) and earlier | 7.00(ABTE.2) |
| | WAX620D-6E | 7.00(ACCN.1) and earlier | 7.00(ACCN.2) |
| | WAX630S | 7.00(ABZD.1) and earlier | 7.00(ABZD.2) |
| | WAX640S-6E | 7.00(ACCM.1) and earlier | 7.00(ACCM.2) |
| | WAX650S | 7.00(ABRM.1) and earlier | 7.00(ABRM.2) |
| | WAX655E | 7.00(ACDO.1) and earlier | 7.00(ACDO.2) |
| | WBE530 | 7.00(ACLE.1) and earlier | 7.00(ACLE.2) |
| | WBE660S | 7.00(ACGG.1) and earlier | 7.00(ACGG.2) |

| Product | Affected model | Affected version | Patch availability |
|---|---|---|---|
| Security router | USG LITE 60AX | V2.00(ACIP.2) | V2.00(ACIP.3) |

## 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://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-os-command-injection-vulnerability-in-aps-and-security-router-devices-09-03-2024