Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Zyxel's Critical Router Vulnerability Exploited via Malicious Cookies

Date of Publication	Admiralty Code	TA Number
September 4, 2024	A1	TA2024338

Summary

First Seen: September 2024
Affected Products: Zyxel APs and Security router
Impact: Zyxel has released security updates to address a critical vulnerability tracked as CVE-2024-7261 affecting multiple models of its business routers and access points (APs). This vulnerability allows unauthenticated attackers to perform OS command injection by sending a specially crafted cookie to the vulnerable devices. If exploited, this flaw could enable attackers to potentially compromise the security and functionality of the affected devices.

CVE

CVE	NAME	AFFECTED PRODUCTS	ZERO-DAY	CISA	PATCH
CVE-2024-7261	Zyxel APs OS Command Injection Vulnerability	Zyxel APs and Security router	✗	✗	✓

Vulnerability Details

#1 Zyxel has patched a critical OS command injection vulnerability, identified as CVE-2024-7261, impacting specific versions of its access points (APs) and security routers. This flaw originates from an input validation issue, where improper handling of user-supplied data allows remote attackers to execute arbitrary commands on the host operating system.

#2 The vulnerability arises from the mishandling of special elements in the "host" parameter within a CGI program. A remote attacker, even without authentication, can exploit this flaw by sending specially crafted cookie to the application, enabling the execution of arbitrary OS commands.

#3 If successfully exploited, this vulnerability could lead to a complete system compromise, underscoring the critical need to apply security patches to safeguard against potential attacks.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-7261	NWA50AX: 7.00(ABYW.1)and earlier, NWA50AX PRO: 7.00(ACGE.1)and earlier, NWA55AXE: 7.00(ABZL.1)and earlier, NWA90AX: 7.00(ACCV.1)and earlier, NWA90AX PRO: 7.00(ACGF.1)and earlier, NWA110AX: 7.00(ABTG.1)and earlier, NWA130BE: 7.00(ACIL.1)and earlier, NWA210AX: 7.00(ABTD.1)and earlier, NWA220AX-6E: 7.00(ACCO.1)and earlier, NWA1123-AC PRO: 6.28(ABHD.0)and earlier, NWA1123ACv3: 6.70(ABVT.4)and earlier, WAC500: 6.70(ABVS.4)and earlier, WAC500H: 6.70(ABWA.4)and earlier, WAC6103D-I: 6.28(AAXH.0)and earlier, WAC6502D-S: 6.28(AASE.0)and earlier, WAC6503D-S: 6.28(AASF.0)and earlier, WAC6552D-S: 6.28(ABIO.0)and earlier, WAC6553D-E: 6.28(AASG.2)and earlier, WAX300H: 7.00(ACHF.1)and earlier, WAX510D: 7.00(ABTF.1)and earlier, WAX610D: 7.00(ABTE.1)and earlier, WAX620D-6E: 7.00(ACCN.1)and earlier, WAX630S: 7.00(ABZD.1)and earlier, WAX640S-6E: 7.00(ACCM.1)and earlier, WAX650S: 7.00(ABRM.1)and earlier, WAX655E: 7.00(ACDO.1)and earlier, WBE530: 7.00(ACLE.1)and earlier, WBE660S: 7.00(ACGG.1)and earlier, USG LITE 60AX: 2.00(ACIP.2)	cpe:2.3:o:zyxel:wbe530_firmware:*:*:*:*:*:*:*:* cpe:2.3:o:zyxel:wax655e_firmware:*:*:*:*:*:*:*:* cpe:2.3:o:zyxel:wac500_firmware:*:*:*:*:*:*:*:* cpe:2.3:o:zyxel:usg_lite_60ax_firmware:*:*:*:*:*:*:*:* cpe:2.3:o:zyxel:nwa1123acv3_firmware:*:*:*:*:*:*:*:*	CWE-78

Recommendations

Update: To mitigate the risk posed by the critical vulnerability CVE-2024-7261, Zyxel has released patches for all affected devices. Users are strongly advised to upgrade their devices as soon as possible to ensure protection against potential exploits.

Vulnerability Management: Implement a robust vulnerability management process to ensure that software and systems are regularly assessed for vulnerabilities and updated with the required security patches. Prioritize critical vulnerabilities identified by security advisories and vendors to mitigate the risk of exploitation by threat actors.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	**TA0002** Execution	**T1588** Obtain Capabilities	**T1588.006** Vulnerabilities
T1059 Command and Scripting Interpreter	**T1584** Compromise Infrastructure	**T1584.008** Network Devices	

Patch Details

Patches addressing the critical vulnerability CVE-2024-7261 have been made available for all affected Zyxel devices. Users are strongly advised to upgrade their devices as soon as possible to ensure protection against potential exploits.

Patch Link:
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

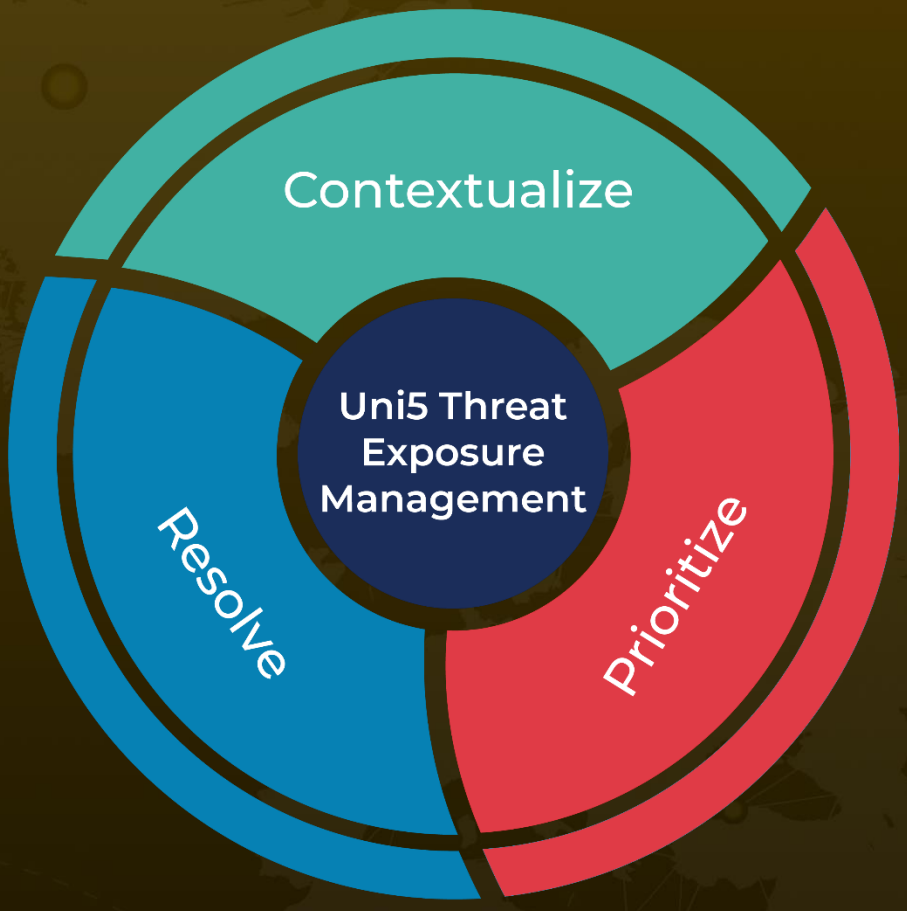
References

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

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

September 4, 2024 • 6:00 AM

More at www.hivepro.com