Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Critical Zyxel CPE Zero-Day Under Active Exploitation

Date of Publication	Admiralty Code	TA Number
January 30, 2025	A1	TA2025025

Summary

First Seen: July 2024
Affected Products: Zyxel CPE series devices
Malware: Mirai
Impact: A critical zero-day vulnerability affecting Zyxel CPE Series devices, tracked as CVE-2024-40891, is currently being actively targeted in the wild. This flaw has remained unpatched since July 2024, leaving devices exposed to exploitation. Researchers have detected botnets, including Mirai, exploiting this flaw, raising the likelihood of large-scale attacks. If successfully leveraged, the vulnerability could allow attackers to execute arbitrary commands on compromised devices, potentially leading to full system takeover, network breaches, and sensitive data leaks.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2024-40891	Zyxel CPE Telnet Command Injection Vulnerability	Zyxel CPE series devices	✓	✗	✗
CVE-2024-40890	Zyxel CPE Command Injection Vulnerability	Zyxel CPE series devices	✗	✗	✗

Vulnerability Details

#1 A critical command-injection vulnerability in Zyxel CPE Series devices tracked as CVE-2024-40891, is being actively exploited in the wild, with no patch currently available. First disclosed in July 2024, this flaw poses a significant risk to affected devices.

#2 The vulnerability resides in the telnet interface of Zyxel CPE devices, allowing unauthenticated attackers to execute arbitrary commands by abusing service accounts such as “supervisor” or “zyuser.” If exploited, it could lead to complete system compromise, unauthorized data access, and network infiltration. Notably, CVE-2024-40891 mirrors the CVE-2024-40890 vulnerability, which targets the HTTP interface instead of telnet, with both vulnerabilities posing significant security risks.

#3 Researchers have identified a strong overlap between IP addresses exploiting CVE-2024-40891 and those linked to the Mirai botnet. Analysis of a recent Mirai variant confirms that this vulnerability has been integrated into certain strains, amplifying the risk of large-scale exploitation. Countries at higher risk include Taiwan, Brazil, India, China, and Thailand. Given the absence of a vendor-issued fix, organizations relying on Zyxel CPE devices must implement immediate mitigation measures to defend against potential intrusions.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-40891	Zyxel CPE Series	cpe:2.3:o:zyxel:cpe:*:*:*:*:*:*:*:*	CWE-78
CVE-2024-40890	Zyxel CPE Series	cpe:2.3:o:zyxel:cpe:*:*:*:*:*:*:*:*	CWE-78

Recommendations

Stay Updated: Keep an eye on Zyxel’s security advisories and apply patches or recommended fixes as soon as they become available to protect your devices.

Implement Temporary Workaround: If turning off Telnet isn’t practical, ensure that only trusted IP addresses can access it. Regularly review and update access control lists (ACLs) to minimize exposure and reduce the risk of unauthorized access.

Monitor Network Traffic for Suspicious Activity: Continuously monitor and filter network traffic for any unusual Telnet requests directed at Zyxel CPE management interfaces. This helps detect potential exploitation attempts and allows for timely response to mitigate threats.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	**TA0001** Initial Access	**TA0002** Execution	**T1588** Obtain Capabilities
T1588.006 Vulnerabilities	**T1059** Command and Scripting Interpreter	**T1078** Valid Accounts	

Patch Details

Since patches are not yet available, stay updated with Zyxel's security advisories and apply patches or recommended fixes as soon as they are released to safeguard your devices.

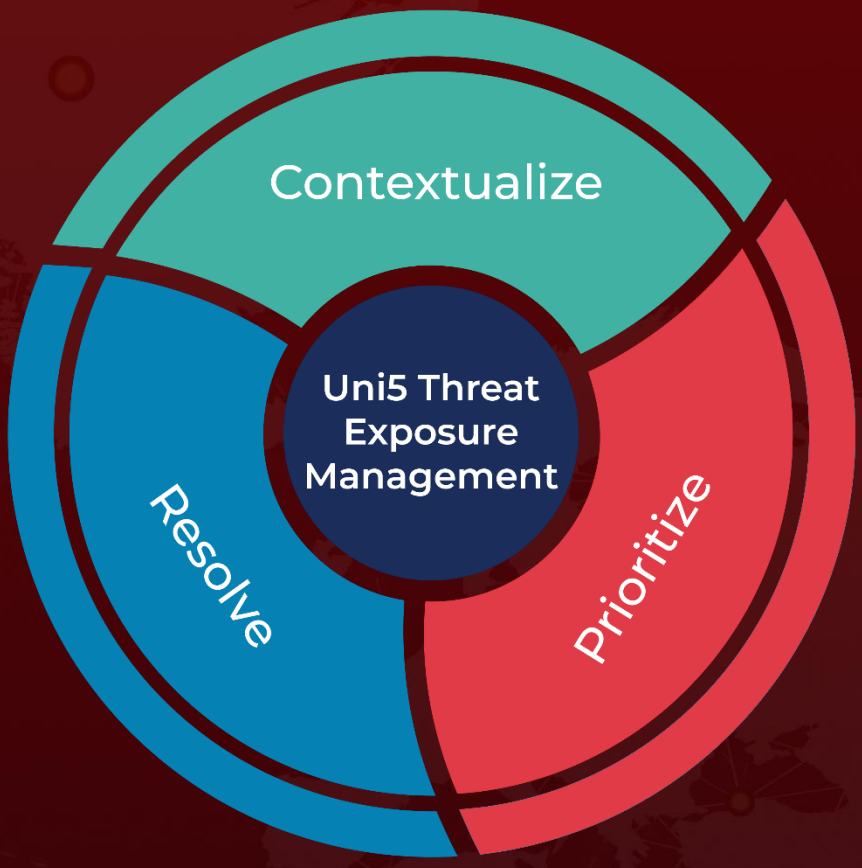
References

https://www.greynoise.io/blog/active-exploitation-of-zero-day-zyxel-cpe-vulnerability-cve-2024-40891

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

January 30, 2025 • 4:40 AM

More at www.hivepro.com