



مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



Critical Vulnerability in Zyxel NAS products

Tracking #:432316250

Date:10-09-2024

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLIGENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability in Zyxel NAS products that could be exploited to execute malicious code on affected systems.

TECHNICAL DETAILS:

Zyxel has addressed a critical command injection vulnerability in its NAS326 and NAS542 devices. This vulnerability, identified as CVE-2024-6342, could allow an unauthorized attacker to execute arbitrary commands on the affected devices. While these devices have reached their end-of-vulnerability-support, Zyxel has released hotfixes to mitigate this risk for customers with extended support.

Vulnerability Details:

- **CVE-2024-6342**
- CVSS Score: **9.8 (Critical)**
- A critical command injection vulnerability exists in the export-cgi program of Zyxel NAS326 and NAS542 devices. This vulnerability could allow an unauthenticated attacker to execute arbitrary commands on the affected devices by sending a specially crafted HTTP POST request.
- Successful exploitation of this vulnerability could result in **remote code execution, data exfiltration, or denial of service.**

Affected model	Affected version	Hotfix availability
NAS326	V5.21(AAZF.18)C0 and earlier	V5.21(AAZF.18)Hotfix-01
NAS542	V5.21(ABAG.15)C0 and earlier	V5.21(ABAG.15)Hotfix-01

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to upgrade the affected versions to the fixed versions at the earliest.

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-nas-products-09-10-2024>