Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Patches Made Available for Vulnerable EoL Zyxel NAS Models

Date of Publication	Admiralty Code	TA Number
June 05, 2024	A1	TA2024215

Summary

Discovered: June 2024
Affected Products: Zyxel NAS326 and NAS542
Impact: Zyxel has released patches to address command injection and remote code execution vulnerabilities in two NAS products. The affected models are NAS326 and NAS542. While three critical flaws have been fixed, issues related to privilege escalation and information disclosure remain unresolved in these end-of-life products. The proof of concept (PoC) for these vulnerabilities is now available.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2024-29972	Zyxel NAS Command Injection Vulnerability	NAS326 and NAS542	✗	✗	✓
CVE-2024-29973	Zyxel NAS Command Injection Vulnerability	NAS326 and NAS542	✗	✗	✓
CVE-2024-29974	Zyxel NAS Remote Code Execution Vulnerability	NAS326 and NAS542	✗	✗	✓
CVE-2024-29975	Zyxel NAS Improper Privilege Management Vulnerability	NAS326 and NAS542	✗	✗	✗
CVE-2024-29976	Zyxel NAS Improper Privilege Management Vulnerability	NAS326 and NAS542	✗	✗	✗

Vulnerability Details

#1

Zyxel Networks has issued an urgent security update for older NAS devices, specifically the NAS326 and NAS542 models, which have reached the end of their life cycle. This update tackles three critical vulnerabilities that could potentially lead to command injection and remote code execution. However, it's important to note that two vulnerabilities related to privilege escalation and information disclosure have not yet been addressed.

#2

CVE-2024-29972 involves a command injection vulnerability in the "remote_help-cgi" CGI program, allowing unauthenticated attackers to execute OS commands via specially crafted HTTP POST requests. CVE-2024-29973 also concerns command injection, this time in the "setCookie" parameter, enabling unauthenticated attackers to execute OS commands through manipulated HTTP POST requests.

#3

CVE-2024-29974 relates to remote code execution in the "file_upload-cgi" CGI program, allowing unauthenticated attackers to run arbitrary code by uploading a crafted configuration file.

#4

Additionally, CVE-2024-29975 pertains to improper privilege management in the SUID executable binary, permitting authenticated local attackers with admin privileges to execute system commands as the root user. Lastly, CVE-2024-29976 involves improper privilege management in the "show_allsessions" command, enabling authenticated attackers to obtain session information, including cookies, of logged-in administrators.

#5

Despite the end of support for both NAS models on December 31, 2023, Zyxel has released fixes for the three critical flaws in versions 5.21(AAZF.17)C0 for NAS326 and 5.21(ABAG.14)C0 for NAS542. This decision was made due to the severity of vulnerabilities CVE-2024-29972, CVE-2024-29973, and CVE-2024-29974. The proof of concept (PoC) for these vulnerabilities is now accessible.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-29972	NAS326 V5.21(AAZF.16)C0 and earlier NAS542 V5.21(ABAG.13)C0 and earlier	cpe:2.3:a:zyxel:nas326:*:*:*:*:*:*:*:* cpe:2.3:a:zyxel:nas542:*:*:*:*:*:*:*:*	CWE-78
CVE-2024-29973	NAS326 V5.21(AAZF.16)C0 and earlier NAS542 V5.21(ABAG.13)C0 and earlier		CWE-78
CVE-2024-29974	NAS326 V5.21(AAZF.16)C0 and earlier NAS542 V5.21(ABAG.13)C0 and earlier		CWE-434
CVE-2024-29975	NAS326 V5.21(AAZF.16)C0 and earlier NAS542 V5.21(ABAG.13)C0 and earlier		CWE-269
CVE-2024-29976	NAS326 V5.21(AAZF.16)C0 and earlier NAS542 V5.21(ABAG.13)C0 and earlier		CWE-269

Recommendations

Update: Update to version 5.21(AAZF.17)C0 for NAS326 and 5.21(ABAG.14)C0 for NAS542 to address the three critical vulnerabilities CVE-2024-29972, CVE-2024-29973, and CVE-2024-29974.

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.

Least Privilege: Adhere to the idea of "least privilege" by giving users only the essential permissions they need for their tasks. This strategy reduces the effects of vulnerabilities related to privilege escalation.

Implement Web Application Firewall (WAF): Deploy a WAF to monitor and filter incoming web traffic. A properly configured WAF can detect and block attempts to exploit the vulnerabilities, providing an additional layer of protection.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	**TA0001** Initial Access	**TA0002** Execution	**TA0004** Privilege Escalation
TA0006 Credential Access	**T1588** Obtain Capabilities	**T1588.006** Vulnerabilities	**T1059** Command and Scripting Interpreter
T1068 Exploitation for Privilege Escalation	**T1539** Steal Web Session Cookie	**T1190** Exploit Public-Facing Application	

Patch Details

Zyxel has issued patches to address the three critical vulnerabilities CVE-2024-29972, CVE-2024-29973, and CVE-2024-29974 in versions:
5.21(AAZF.17)C0 for NAS326 and 5.21(ABAG.14)C0 for NAS542

Links:
https://www.zyxel.com/global/en/support/download

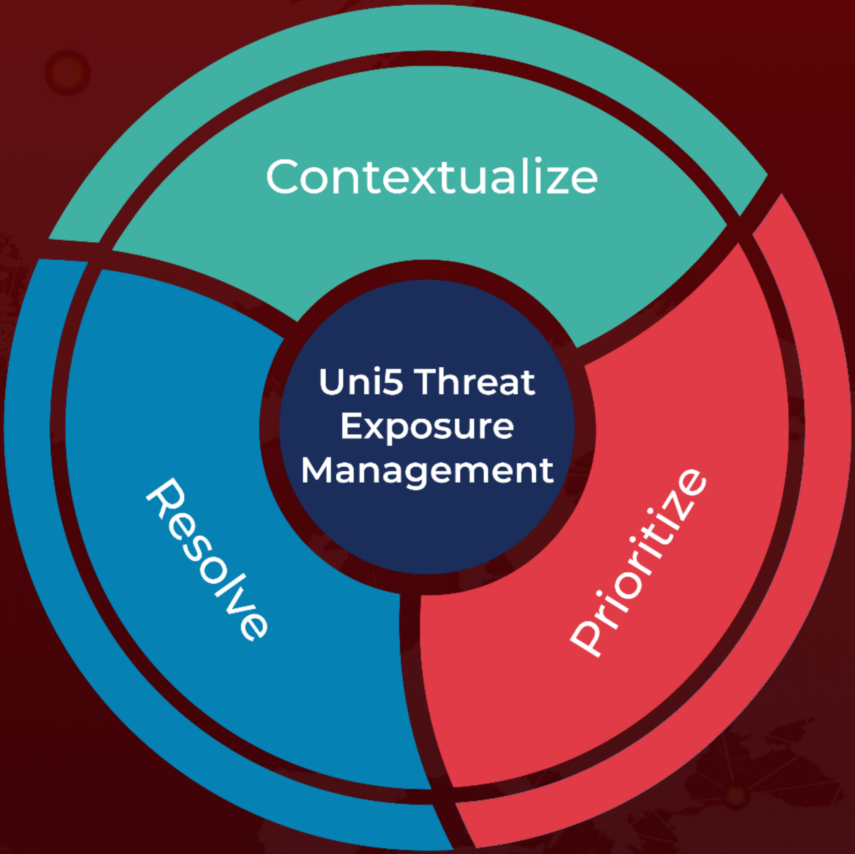
References

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

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

June 05, 2024 • 6:00 AM

More at www.hivepro.com