CYBER ADVISORY

Cal OES
GOVERNOR'S OFFICE
OF EMERGENCY SERVICES

CALIFORNIA CYBERSECURITY INTEGRATION CENTER

CYBER ADVISORY

TLP:CLEAR
04 June 2024

Zyxel NAS Vulnerabilities

Zyxel | NAS | RCE | Critical Vulnerabilities

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of a critical vulnerabilities known as CVE-2024-29972, CVE-2024-29973, CVE-2024-29974, CVE-2024-29975, and CVE-2024-29976.[1] The vulnerabilities affect Zyxel NAS products NAS326 version V5.21(AAZF.16)C0 and earlier and NAS542 version V5.21(ABAG.13)C0 and earlier.[2] Exploitation of the vulnerabilities may allow an authenticated attacker to conduct command injection and remote code execution, (RCE) on the affected devices.[3]

CVE	Description of Vulnerability	Patch Availability
CVE-2024-29972	Command injection flaw in the CGI program ('remote_help-cgi') allowing an unauthenticated attacker to send a specially-crafted HTTP POST request to execute OS commands using a NsaRescueAngel backdoor account that has root privileges.	Patch is Available
CVE-2024-29973	Command injection flaw in the 'setCookie' parameter, allowing an attacker to send a specially-crafted HTTP POST request to execute OS commands.	Patch is Available
CVE-2024-29974	Remote code execution bug in the CGI program ('file_upload-cgi'), allowing an unauthenticated attacker to upload malicious configuration files on the device.	Patch is Available
CVE-2024-29975	Improper privilege management flaw in the SUID executable binary allowing an authenticated local attacker with admin rights to execute system commands as the "root" user.	Patch is not Available
CVE-2024-29976	Improper privilege management problem in the 'show_allsessions' command, allowing an authenticated attacker to obtain session information, including active admin cookies.	Patch is not Available

Table 1: Zyxel NAS Vulnerabilities

The Cal-CSIC recommends to immediately apply patches to the affected Zyxel NAS products to mitigate against the most critical vulnerabilities. Cal-CSIC additionally recommends using another product as the affected products have reached end of life (EOL) for support as of 31 December 2023.

For further information on applying patches and information on Zyxel NAS EOL status, please refer to Zyxel Networks Community.

WARNING: This document is the exclusive property of the California Cybersecurity Integration Center (CAL-CSIC) and abides by Traffic Light Protocol (TLP) standards for distribution purposes. It may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 6250, et seq.). Recipients must control, store, handle, transmit, distribute, and dispose of this product in accordance with the TLP standard relating to shared intelligence. Do not release to the public, media, or other personnel who do not have a valid need-to-know without prior approval of an authorized CAL-CSIC official.

Organization, Source, Reference, and Dissemination Information

Organization Description	California Government Code § 8586.5 established the California Cybersecurity Integration Center (Cal-CSIC) as the central organizing hub of state government's cybersecurity activities, including information sharing, intelligence analysis, incident response, and overarching cybersecurity strategy. The Cal-CSIC is responsible for reducing the likelihood and severity of cyber incidents that could damage California's economy, critical infrastructure, and public or private sector networks in our state.
Customer Feedback	If you need further information about this issue, contact the Cal-CSIC at our email address CalCSIC@caloes.ca.gov or by telephone at (833) REPORT1. To help us identify ways to better assist you, please submit feedback calcsic@caloes.ca.gov.
Source Summary Statement	This report was compiled from a variety of sources, predominately open-source reporting.
Handling Caveats	**Traffic Light Protocol (TLP):** Recipients may share TLP:CLEAR information with the world; there is no limit on disclosure. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.
Information Needs	*HSEC 1.1; HSEC 1.2; HSEC 1.5; HSEC 1.8; HSEC 1.10; STAC KIQ 1.1; KIQ 1.2; KIQ 1.3; KIQ 1.4; KIQ 1.5*

[1] Bleeping Computer; "Zyxel issues emergency RCE patch for end-of-life NAS devices;" https://www.bleepingcomputer.com/news/security/zyxel-issues-emergency-rce-patch-for-end-of-life-nas-devices/; accessed 04 June 2024

[2] Outpost 24; "Five new vulnerabilities found in Zyxel NAS devices (including code execution and privilege escalation);" https://outpost24.com/blog/zyxel-nas-critical-vulnerabilities/; accessed 04 June 2024

[3] Zyxel Networks; "Zyxel security advisory for multiple vulnerabilities in NAS products;" https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-nas-products-06-04-2024; accessed 04 June 2024

WARNING: This document is the exclusive property of the California Cybersecurity Integration Center (CAL-CSIC) and abides by Traffic Light Protocol (TLP) standards for distribution purposes. It may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 6250, et seq.). Recipients must control, store, handle, transmit, distribute, and dispose of this product in accordance with the TLP standard relating to shared intelligence. Do not release to the public, media, or other personnel who do not have a valid need-to-know without prior approval of an authorized CAL-CSIC official.