

# Release Note

## **NAS326**

Version 5.21(AAZF.18)C0

June 17, 2024

Copyright © 2024 Zyxel and /or its affiliates. All Rights Reserved.

**NAS326**  
**Release V5.21(AAZF.18)C0**

**Release Notes**

**Supported Platforms:**

ZyXEL NAS326

**Release Package:**

File name	
521AAZF18C0.bin	NAS Firmware Package for standard version
521AAZF18C0.pdf	Firmware release note

### **Design Limitations:**

Note: Design Limitations described the system behavior or limitations in current version. They will be created into knowledge base.

1. The new version of the package does not support retrieving Google Drive capacity.

**Known Issues:**

1. Due to limitations with filtered characters, a timezone containing '&' cannot be set up

## **Features**

### **Modification in V5.21(AAZF.18)C0 | June 17, 2024**

[Bug fix]

- Upgrade GoogleDriveClient package from 0.5.0 to 0.5.3 version to fix users' google drive account sync issue.
- Hide capacity of Google drive on NAS GUI because new version package does not support to get google drive capacity.

### **Modification in V5.21(AAZF.17)C0 | May 10, 2024**

[Bug fix]

- CVE-2024-29972 (Command injection vulnerability in the CGI program "remote\_help-cgi")
- CVE-2024-29973 (Command injection vulnerability in the command "setCookie")
- CVE-2024-29974 (Remote code execution (RCE) vulnerability in the CGI program "file\_upload-cgi")

### **Modification in V5.21(AAZF.16)C0 | January 10, 2024**

[Bug fix]

- Zyxel-SI-1517 [Vulnerability] Multiple post-auth blind code injection in NAS326.
  - Issue 1 (SEC-BUGPROVE-2023-11-260923-091554)
- Filter more characters on NAS GUI web pages. (File Browser, Backup Planner)

### **Modification in V5.21(AAZF.15)C0 | November 8 2023**

[Bug fix]

- Zyxel-SI-1497 [Vulnerability] Authentication bypass and pre-authentication command injection vulnerabilities in NAS
- Zyxel-SI-1501 [Vulnerability] Multiple remote code execution vulnerabilities in NAS
- Zyxel-SI-1509 [Vulnerability] Pre-auth command injection vulnerability in NAS
- Zyxel-SI-1510 [Vulnerability] Multiple post-authentication OS command injections in NAS326
- Zyxel-SI-1517 [Vulnerability] Multiple post-auth blind code injection in NAS326
  - Issue 2 (SEC-BUGPROVE-2023-12-260923-091622)
  - Issue 3 (SEC-BUGPROVE-2023-13-260923-091646)

- Zyxel-SI-1519 [Vulnerability] Authentication bypass and command injection vulnerabilities in NAS326
- Filter more characters on some NAS GUI pages.
  - Filter 10 characters : `', '\$', '^', '&', '\\', ';', '"', "'", '<', '>'

#### **Modification in V5.21(AAZF.14)C0 | June 1 2023**

[Bug fix]

- Create and Delete disk group with 2 disks will show 500 Internal Server Error.
- [SI-1480] Zyxel-SI-1480 [Vulnerability] Pre-authentication RCE in NAS326 (also affect NAS540, NAS542).
- [SI-1481] Zyxel-SI-1481 [Vulnerability] Pre-authentication RCE in NAS542 (also affect NAS326, NAS540).

#### **Modification in V5.21(AAZF.13)C0 | May 11 2023**

[Bug fix]

- [Zyxel-SI-1474] [Vulnerability] Post-authentication command injection in NAS326. The value of "Time server address" only accepts the characters :
- '-', ':', '0'~'9', 'A'~'Z', 'a'~'z'
- [eITS#230201044][356032] NAS542 / percentage symbol in user's password cause system folder full access via FTP.

#### **Modification in V5.21(AAZF.12)C0 | Aug 16 2022**

[Enhancement]

- Remove NAS starter utility related information.

[Bug fix]

- [Vulnerability] Format string vulnerability
- Remove nsuagent and do not support NAS starter utility.)
- Users can't enable PHP-MySQL-phpMyAdmin and other 4 packages(Logitech® Media Server, WordPress, Gallery, ownCloud) on NAS GUI App Center.

#### **Modification in V5.21(AAZF.11)C0 | May 30 2022**

[Enhancement]

- Force upgrade Certificate(CA) from old RSA public key to new one.(4096 bits)

Copyright © 2024 Zyxel and /or its affiliates. All Rights Reserved.

- Disable CUPS. Remove printer server service page and related information on help page.
- Upgrade netatalk from 3.1.7 to 3.1.13 .

[Bug fix]

- NAS326 / LAN Port 100 MBit/s after restart.
- Fix possible infinite loop in BN\_mod\_sqrt.

#### **Modification in V5.21(AAZF.10)C0 | April 15 2021**

[Enhancement]

- Upgrade Twonky Server to 8.5.2 .

[Bug fix]

- CVE-2020-13848 Portable UPnP SDK (aka libupnp) 1.12.1 and earlier allows remote attackers to cause a denial of service (crash) via a crafted SSDP message.
- Fix CVE-2020-9054. RCE of FTP login.

#### **Modification in V5.21(AAZF.9)C0 | Jun 12 2020**

[Bug fix]

- Fix NAS Remote access via backdoor. Hackers need to know NAS account/password(admin or root) first. Then they use it to login to NAS's web application and open specified URL to enable Telnet feature. An unprivileged user account 'admin' can generate a new password for the user account 'NsaRecureAngel' via Telnet. Then, the password can be used with the user 'NsaRescureAngel' to access the device via Telnet with root privileges.
- Fix if total size (unallocated capacity + current volume size) is larger than 16 TB (16383 GB), Editing volume size by clicking "MAX" button will make volume size larger than 16 TB. After applying this setting, user cannot login web GUI.

#### **Modification in V5.21(AAZF.8)C0 | Mar 20 2020**

[Bug fix]

- Fix Vulnerability issue from remote unauthenticated attacker.
  - CVE-2018-11160 (Netatalk)
- Fix rhost name buffer overflow issue.
  - CVE-2020-8597

[Enhancement]

- Modify filtering characters of login password.  
Filter 9 characters as below:  
\" ' ` < > ^ \$ &
- Modify filter emoji emoticons:  
\\u1F60-\\u1F64, \\u2702-\\u27B0, \\u1F68-\\u1F6C,  
\\u1F30-\\u1F70, \\u2600-\\u26ff

**Modifications in V5.21(AAZF.7)C0 | Feb 24 2020**

[Bug fix]

- Fix Samba issue:
  - CVE-2014-3560 - CVE-2015-0240 - CVE-2016-2123
  - CVE-2017-7494 - CVE-2017-14746
- Fix RCE(remote code execution) attack.
  - CVE-2020-9054
- Change client ID and secret of YouTube upload.

[Package]

- [myZyXELcloud-Agent] update certification.

**Note**

*If you cannot login the web interface with original password after firmware update is finished, please press the hardware reset button at the back of NAS for 2 seconds, and you will hear one beep sound, then release the hardware reset button. This resets the NAS's IP address and password to the default setting. (admin/1234)*

**Modification in V5.21(AAZF.6)C0 | Sep 26 2019**

[Enhancement]

- Enhancement the patch for networking vulnerabilities to fix:
  - CVE-2019-11477 - CVE-2019-11478
  - CVE-2019-11479

[Bug fix]

- Fix Time zones and DST issue for Russia.
- Fix Monthly power schedule issue.



**Modifications in V5.21 (AAZF. 4)C0 | Jun 13 2019**

[Enhancement]

- Apply the patch of kernel to support all CPU version.

**Modification in V5.21(AAZF.3)C0 | Nov 15 2018**

[Bug fix]

- Fix power schedule issue.
- Fix File Browser issue.

**Modification in V5.21(AAZF.2)C0 | Jun 21 2018**

[Bug fix]

- Fix sys log issue.
- Fix NFS problem.
- Remove "Hot swapping" related information.
- Modify the schedule time issue.
- Modify default folder setting.

**Modification in V5.21(AAZF.1)C0 | May 26 2017**

[Enhancement]

- Enhance the API of backup planner to verify the session before proceeding with the procedure.
- Enhance the implementation of backup planner to eliminate the risk of command injection.

**Modification in V5.21 (AAZF0. C0) | May 4 2017**

[Bug fix]

- Apply the patch to fix CVE-2016-10229
- Upgrade libupnp to fix CVE-2016-6255 and CVE-2016-8863
- Fix the file browser API accepts relative path as the arguments which causes security problem.

[Enhancement]

- Upgrade ftp module for security consideration.
- Now users can play media files on Twonky GUI from remote WAN, ex.dydns.
- Upgrade Twonky media server to 8.3.19

- Turn off TLSv1.0 and TLSv1.1 and revise the cipher suite to enhance the security.
- Force the admin account to modify the password from the default value.

[Package]

- [ownCloud] Upgrade to 7.0.15
- [pyLoad] Fix "package "Pyload" won't work"

**Modification in V5.20(AAZF.3)C0 | Nov 17 2016**

[Bug fix]

- NAS sync client cannot see folders
- Two external HDD connected cause no HDD can detect and backup job fail.
- The portal users of information display error information when the myZyxelCloud is installed in some volume other than system volume.
- Mac OS 10.12 fails to backup data to NAS through Time Machine.
- File Browser fails to restore multiple files from recycle-bin.
- Automatically summer time can't activate
- Time Zone change issue
- User Edit / Remove / Add fail in some case after upgrading to v5.20
- Dropbox Key Login failed.
- User Modify default password by admin after reboot the password can't be set.
- Time Machine is disabled after reboot.
- File Browser Copy Issue
- File Browser delete cause error message
- File Browser delete something in recycle bin cause loop
- Click "Clean all recycle bin now", some of recycle bin would not clean the files which in the recycle bin.
- Create new share and publish to Media Server ignore the setting.

**Modification in V5.20(AAZF.0)C0 | Sep 6 2016**

[Enhancement]

- New GUI

- New behavior of user/group/share management.
- Upgrade Twonky Media Server to 8.2
- Remove the 2 GB upload limitation of file browser on Web GUI.
- Twonky with HTML5 player

[Bug fix]

- Refine the mechanism to check looped folder.
- Correct the mechanism in Auto Upload to determine if a path is a subfolder of another path.
- The privilege of shares with any ' or " in its name can't be modified.

[Package]

- [All Package] App Center on Desktop
- [DropboxClient] Support Dropbox two way sync
- [DropboxClient] Dropbox synchronization for all sub folders.
- [DropboxClient] Fix DropboxClient cannot detect remote-deleted files.
- [NZBGet,PHP,SqueezeCenter,Transmission,WordPress,Gallery,ownCloud] Rebuilt UPnP database when NAS reset to default.

**Modification in V5.11(AAZF.4)C0 | Jun 3 2016**

[Enhancement]

- Revise the implementation of GUI so that the behavior of clicking myZyXEcloud button on Desktop won't be blocked by web browser.

[Bug fix]

- Fix the NAS IP incorrect in 5 minutes after changing NAS hostname

[Package]

- **[PHP]**Rebuild php, because open ssl be upgraded.
- **[NFS]**Fixed Bug: NFS configure file does not be removed when removing NFS.

**Modification in V5.11(AAZF.3)C0 | Mar 8 2016**

[Enhancement]

- Apply the patch of glibc to fix CVE-2015-7547

**Modification in V5.11(AAZF.2)C0 | Feb 16 2016**

[Bug fix]

- Fix FTP client can't login issue

**Modification in V5.11(AAZF.1)C0 | Feb 1 2016**

[Bug fix]

- The file browser of Web GUI fails to decompress files if there exists quota limitation of the login user.
- Sometimes the icons on desktop are gone when login.
- Revise the log "Failed unknown login attempt (incorrect password or inexistent username)" when the Rsync task fails to authenticate.

[Enhancement]

- Enhance how the GUI determine if the email address user entered is valid.
- Apply the patch of Linux kernel to fix CVE-2016-0728.

**Enhancement in V5.11(AAZF.0)C0 | Jan 15 2016**

[Enhancement]

- Refine the algorithm of password strength determination.
- The password of 14 consecutive 'A' is determined as strong password which is wrong.
- Adjust the local port range to avoid port conflicts between services.
- Let the Twonky GUI sort the files by track number in folder view.
- User searching supports cloud users.
- Updated some missing translations.
- Fine tune some GUI behavior
- Speedup the login process of WebDAV.
- Show the icons after installed package on GUI.
- Cloud users now are represented with their email account

[Bug fix]

- Hide the group item in the session table. It's meaningless.
- Deleting a share always turn on the media server even when it's been turned off.

- Time zone spelling correction. (Pitori" to "Pretoria")
- The Music/Video/Photo icon in the desktop-style page doesn't work on Safari.
- The icon for cloud users is created.
- The login time displayed in the session information is negative in German.
- MAC OS X 10.11 and Safari Media Icon fails open
- Media Server activate automatic if delete share
- Half icon with smaller monitor
- Status Center File Transfer show wrong values
- After Restart admin must be login once for backup job from other NAS
- Users can't access the external volume through WebDAV if they just hot plug USB storage without entering the Web GUI.
- Correct the address in the link in the Webpage that helps users to link to the device after firmware upgrading.
- Add the firmware version in the message after firmware upgrading.
- Show the IPv6 information when it's from AUTO-IP, which means there's no IPv6 DHCP in the environment.
- The icons on the desktop page can't be displayed correctly after dragging.
- The system fails to boot up after setting the network to static through NSU.
- The DHCP client ask for IP with model name instead of hostname.
- The folders created though WebDAV can't be deleted through samba.

**Enhancement in V5.10(AAZF.0)C0 | Oct 30 2015**

[Initial version]