QNAP provides an emergency warning about NAS device attack trends, showing how to secure NAS devices

NAS (Network Attached Storage), also known as a network hard drive, is a device that is installed to serve the needs of storing or accessing data.

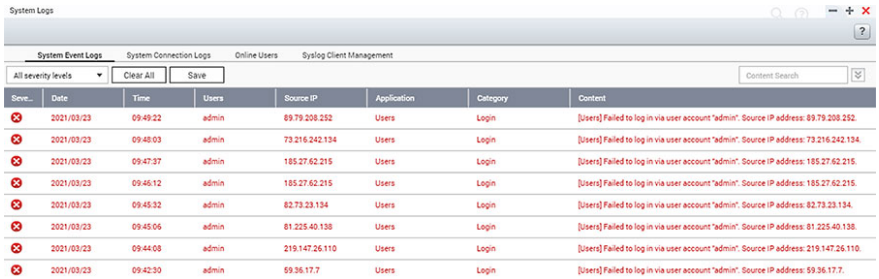
NAS is considered the leading secure personal data storage solution for those who do not want to use cloud storage services. However, this does not mean that NAS devices are completely 'immune' to security threats.

QNAP is the world's leading NAS manufacturer. Recently, QNAP has issued urgent notice related to the attacks targeting its NAS devices worldwide. This offensive trend is constantly increasing at an alarming rate. At the same time, QNAP also urges users to immediately strengthen appropriate security measures as soon as possible.

In these typical attacks, the threat agent often uses automated tools to log in to NAS devices connected to the Internet using passwords generated locally, or from a list of credentials. has been compromised before.

A warning from QNAP said: ' *Recently QNAP received many reports from users about hackers trying to log in to their QNAP device using brute-force attacks. In it, hackers will try every possible combination of passwords to break into the QNAP device user account . If a user uses a simple, weak, or predictable password (such as' abc123 'or' 123456 '), a hacker can easily access their NAS device* '.

Essentially, hacking into the NAS account gives the hacker the right to access and steal sensitive documents or deploy malware on the victim's system.



How to secure the QNAP NAS device

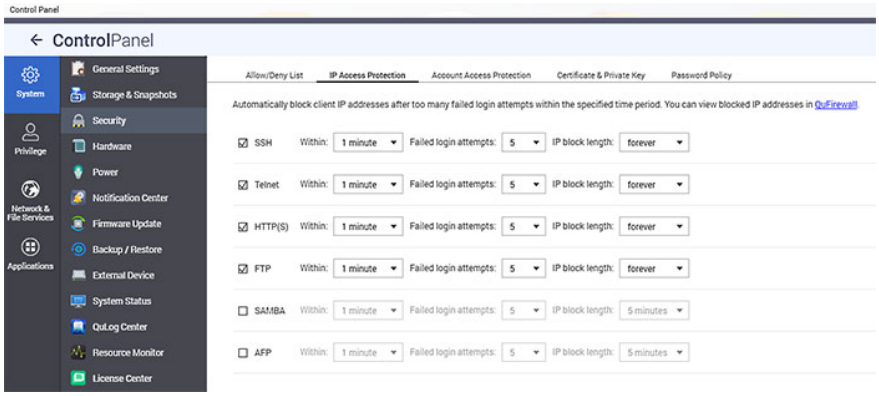
QNAP recommends that customers secure their NAS devices by changing the default access port number, using strong passwords for their accounts, enabling password policies, and disabling the administrator account. is targeted in these ongoing attacks.

Before disabling the admin account, you will have to create a new system admin account by going to **Control Panel> Users** .

You will then be able to disable the default ' **admin** ' administrator account on QNAP NAS devices running QTS version 4.1.2 or higher with these steps:

1. Navigate to **Control Panel> Users** and edit the " **admin** " account profile .
2. Check the option " **Disable this account** " and click " **OK** ".

Alternatively, you can also configure the NAS device to block IP addresses automatically after multiple login attempts. Do this by customizing the device's security settings from the **NAS Control Panel** tab **> System> Security> IP Access Protection** .



QNAP NAS owners should also go through the following checklist to secure their NAS device and check for malware:

1. Change passwords for all accounts on the device
2. Remove unknown user accounts from the device
3. Make sure the device's firmware is up to date and that all apps are running on the latest version as well.
4. Remove unknown or unused applications from the device
5. Install QNAP MalwareRemover application through App Center function
6. Set access control list for the device (**Control panel -> Security -> Security level**)

You finished reading the article "**QNAP provides an emergency warning about NAS device attack trends, showing how to secure NAS devices**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.