OVERLAND TANDBERG

Corporate Headquarters
2633 Camino Ramon, Suite 325
San Ramon, CA 94583
408.283.4700

11/16/2023

Dear valued RDX QuikStation customers,

We are pleased to announce the release of a new set of software patches for the RDX QuikStation 4 and QuikStation 8 firmware. These patches are designed to enhance the security of our product by addressing a number of Common Vulnerabilities and Exposures (CVE) issues. The patches will successfully install on any QuikStation running the 3.x.x.x firmware, but we do recommend always using the most recent firmware release (currently 3.2.1.2 as of the release of these patches).

However, please note that to implement these crucial security updates, the Web User Interface (UI) will be disabled when the product is not actively being configured. This measure is necessary to ensure the robustness of the security enhancements and to maintain the integrity of the system.

We understand that this change may affect your user experience, and we appreciate your understanding and cooperation. Our team is committed to providing you with a secure and reliable product, and we believe that this update is a significant step towards that goal.

A security scan of RDX QuikStation 4 or QuikStation 8 before applying the patch and disabling the Web interface will reveal the following security concerns:

- OpenSSL vulnerability (CVE-2022-2068)
- OpenSSL vulnerability (CVE-2022-1292)
- Obsolete Version of PHP
- OpenSSL vulnerability (CVE-2021-3711)
- PHP Vulnerability: CVE-2022-31625
- PHP Vulnerability: CVE-2021-21703
- PHP Vulnerability: CVE-2021-21708
- X.509 Certificate Subject CN Does Not Match the Entity Name
- PHP Vulnerability: CVE-2022-31626
- OpenSSL vulnerability (CVE-2021-3712)
- PHP Vulnerability: CVE-2020-7069
- TLS/SSL Server Supports DES and IDEA Cipher Suites
- Untrusted TLS/SSL server X.509 certificate
- Missing Http Only Flag From Cookie
- Missing Secure Flag From SSL Cookie
- OpenSSL vulnerability (CVE-2022-0778)
- OpenSSL vulnerability (CVE-2021-23840)
- PHP Vulnerability: CVE-2021-21702
- PHP Vulnerability: CVE-2019-11048
- PHP Vulnerability: CVE-2021-21705

- PHP Vulnerability: CVE-2020-7071
- PHP Vulnerability: CVE-2020-7070
- OpenSSL vulnerability (CVE-2022-2097)
- PHP Vulnerability: CVE-2021-21707
- Click Jacking
- PHP Vulnerability: CVE-2021-21704
- OpenSSL vulnerability (CVE-2021-3449)
- OpenSSL vulnerability (CVE-2021-23841)
- OpenSSL vulnerability (CVE-2020-1971)
- OpenSSL vulnerability (CVE-2022-4450)
- OpenSSL vulnerability (CVE-2022-4304)
- OpenSSL vulnerability (CVE-2023-0286)
- OpenSSL vulnerability (CVE-2023-0215)
- PHP Vulnerability: CVE-2022-31630
- PHP Vulnerability: CVE-2022-37454
- PHP Vulnerability: CVE-2022-31628
- PHP Vulnerability: CVE-2022-31629
- OpenSSL vulnerability (CVE-2021-4160)
- Self-signed TLS/SSL certificate
- TLS Server Supports TLS version 1.0
- TLS/SSL Server is enabling the BEAST attack
- TLS/SSL Weak Message Authentication Code Cipher Suites
- PHP Vulnerability: CVE-2020-7068
- TLS/SSL Server Is Using Commonly Used Prime Numbers
- TLS/SSL Server Supports The Use of Static Key Ciphers
- TLS Server Supports TLS version 1.1
- ICMP timestamp response
- TCP timestamp response
- TLS/SSL Server Does Not Support Any Strong Cipher Algorithms

After applying the patch and disabling the Web UI, the only remaining open issue is:

- ICMP timestamp response

We expect to address that issue with an upcoming RDX QuikStation firmware release.

Your Overland-Tandberg Team

RDX® QuikStation®
Security Patch Instructions

November 2023

Preface

This Product Information Bulletin announces the release of a new set of software patches for the RDX QuikStation 4 and QuikStation 8 firmware. These patches are designed to enhance the security of the QuikStation by addressing a number of Common Vulnerabilities and Exposures (CVE) issues. The patches will successfully install on any QuikStation running the 3.x.x.x firmware, but we do recommend always using the most recent firmware release (currently 3.2.1.2 as of the release of these patches).

Process Overview

The use of Bitvise as a tool in this document is intended to facilitate ease of use. Use Bitvise on Windows systems to ease the process of generating SSH key pairs and copying files to the QuikStation, or use the tools you're comfortable with. Either will work.

Here is a high level overview of the general steps required to apply the patch:

1. Generate SSH key-pairs
2. Upload SSH key to QuikStation
3. Upload patch file
4. Extract patch scripts from patch file
5. Set permissions on the scripts
6. Run patch scripts

Obtain the Required QS-Patch.tar file

The use of Bitvise as a tool in this document is intended to facilitate ease of use. Use Bitvise on Windows systems to ease the process of generating SSH key pairs and copying files to the QuikStation, or use the tools you're comfortable with. Either will work.

1. The necessary scripts are in the "QS-Patch.tar" file. They are:
   - "QS-security-patch.sh"
   - "webinterface.sh"
2. Download the file from here.

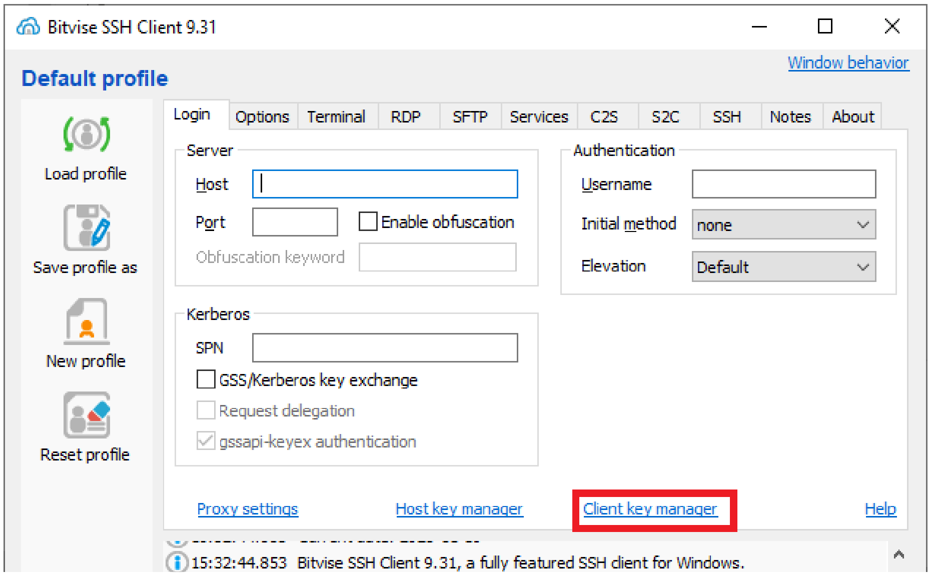
SSH Client Prerequisites

Download Bitvise and install on Windows

1. Use the Bitvise client to assist with SSH connections and key management. The latest release can be found here: https://www.bitvise.com/ssh-client-download
2. Install Bitvise using all the default settings.

Generate and export SSH public/private keypair

1. Launch Bitvise.
2. Click on Client Key Manager.



Bitvise SSH Client 9.31

Default profile

Window behavior

Server

Host

Port

☐ Enable obfuscation

Obfuscation keyword

Authentication

Username

Initial method: none

Elevation: Default

Kerberos

SPN

☐ GSS/Kerberos key exchange

☐ Request delegation

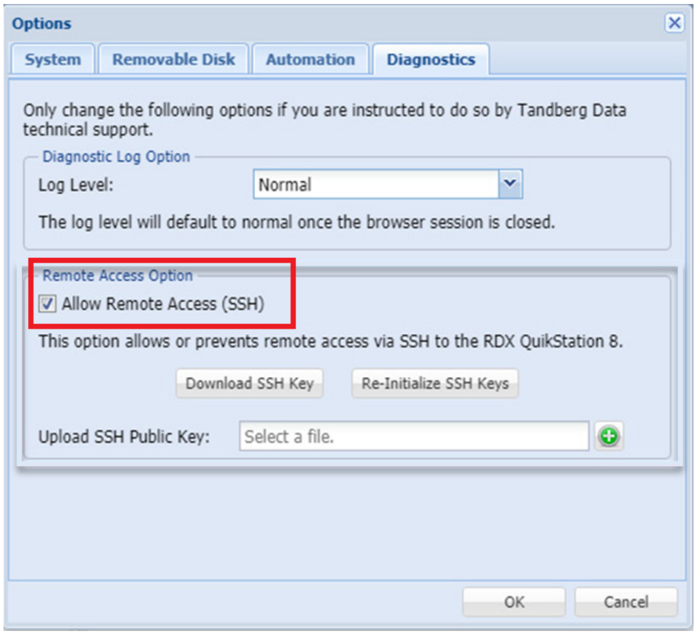
☑ gssapi-keyex authentication

15:32:44.853 Bitvise SSH Client 9.31, a fully featured SSH client for Windows.

1. Generate a key by clicking “Generate New”.
2. In the window that pops up, enter a passphrase and click “Generate”.
3. Select the Key you just generated and click the “Export” button.
4. Select the OpenSSH format and click “Export”.
5. Place the key where you can access it later.

Enable remote SSH access to the QuikStation

1. From the Remote Management Console main menu for the QuikStation, select **System Settings** > **Options**.
2. Under the **Diagnostics** tab, select the **Allow Remote Access (SSH)** option and select **OK** to permit the use of SSH to access the RDX QuikStation.



Options

Only change the following options if you are instructed to do so by Tandberg Data technical support.

Diagnostic Log Option

Log Level: Normal

The log level will default to normal once the browser session is closed.

Remote Access Option

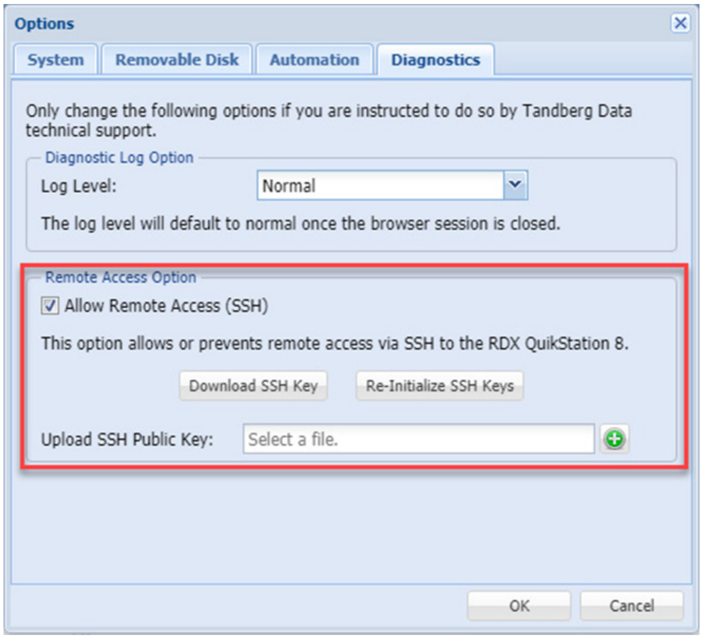
☑ Allow Remote Access (SSH)

This option allows or prevents remote access via SSH to the RDX QuikStation 8.

Upload SSH Public Key: Select a file.

Upload the Public SSH Key to QuikStation

1. From the Remote Management Console main menu for the QuikStation, select **System Settings** > **Options**.
2. Switch to the **Diagnostics** tab.
3. Click the green plus icon to the right of **Upload SSH Public Key**.
4. Using the file explorer that pops up, navigate to the location where you saved the public key and select **Open**.
5. Click **OK** again to close the System Settings options dialog box and upload the key.



Only change the following options if you are instructed to do so by Tandberg Data technical support.

Diagnostic Log Option

Log Level: Normal

The log level will default to normal once the browser session is closed.

Remote Access Option

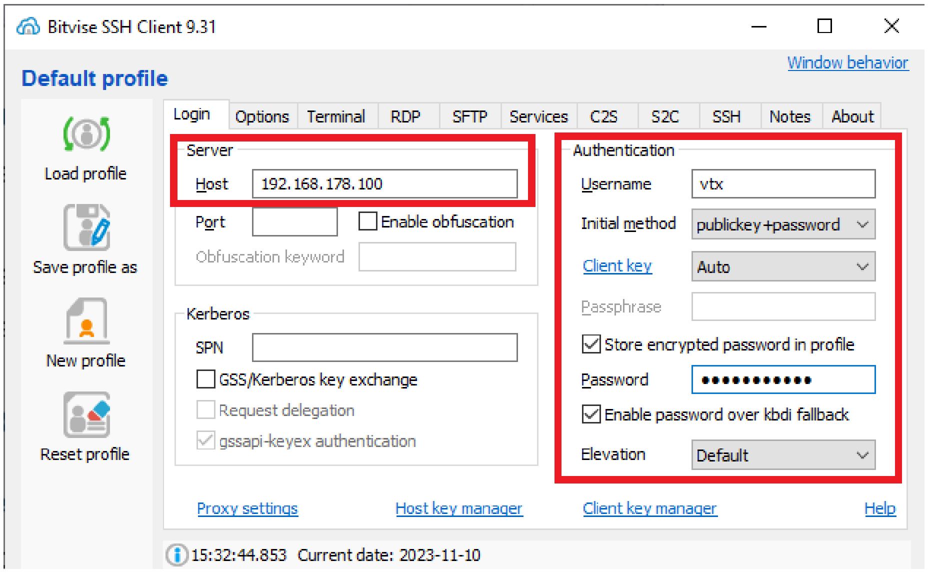
☑ Allow Remote Access (SSH)

This option allows or prevents remote access via SSH to the RDX QuikStation 8.

Upload SSH Public Key: Select a file.

Connect to QuikStation

1. Set the Host to the <**ip address of your QuikStation**>
2. In the Authentication Section, set the Username to **vtx**
3. Set the Initial method to **publickey+password**
4. Set Client key to **Auto**



Server

Host 192.168.178.100

Port

☐ Enable obfuscation

Obfuscation keyword

Kerberos

SPN

☐ GSS/Kerberos key exchange

☐ Request delegation

☑ gssapi-keyex authentication

Authentication

Username vtx

Initial method publickey+password

Client key Auto

Passphrase

☑ Store encrypted password in profile

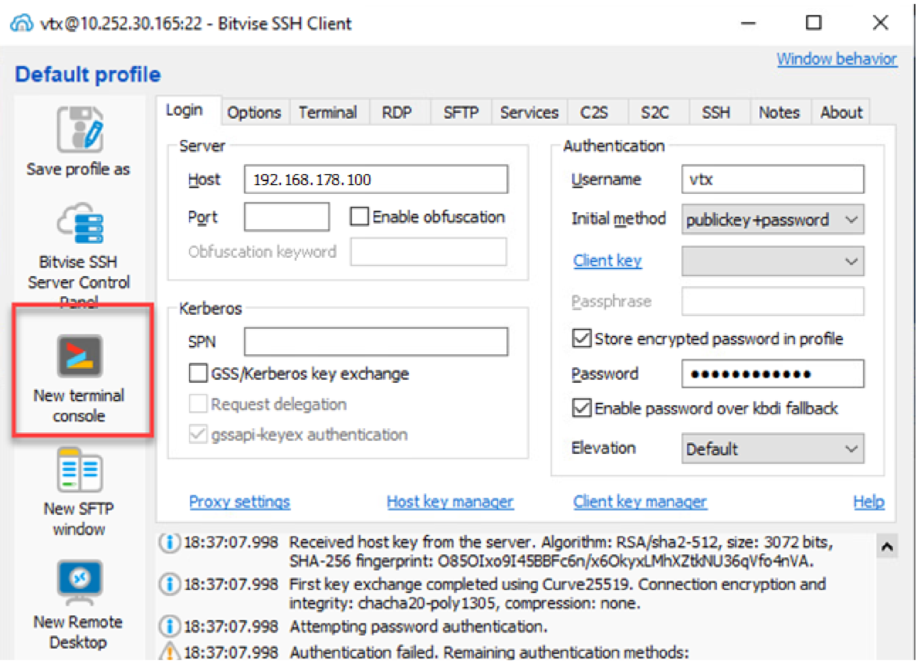
Password ●●●●●●●●●●●

☑ Enable password over kbdi fallback

Elevation Default

15:32:44.853 Current date: 2023-11-10

5. Select **Log In**, then **Accept and Save** to make the SSH connection to QuikStation.
6. When prompted, enter the passphrase you used when generating the key.
7. Once the client is connected, you will see additional icons on the left of the window, such as **New terminal console** and **New SFTP window**.



Server
Host: 192.168.178.100
Port:
□ Enable obfuscation
Obfuscation keyword:

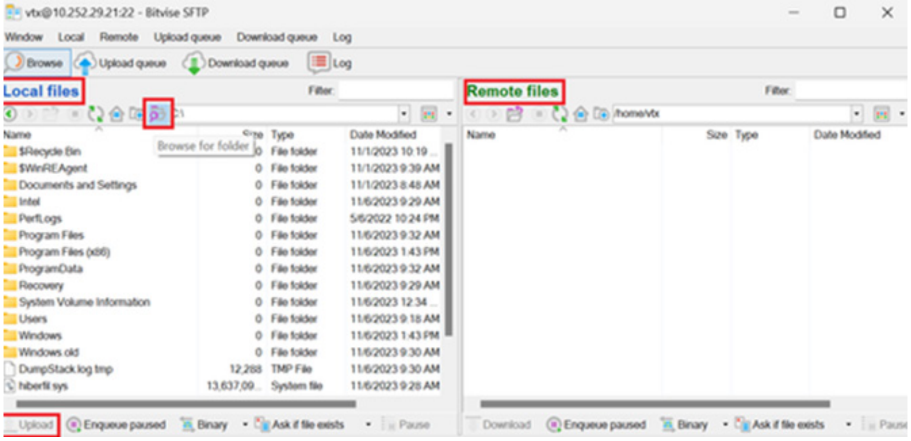
Kerberos
SPN:
□ GSS/Kerberos key exchange
□ Request delegation
☑ gssapi-keyex authentication

Authentication
Username: vtx
Initial method: publickey+password
Client key:
Passphrase:
☑ Store encrypted password in profile
Password: ●●●●●●●●●●●●
☑ Enable password over kbdi fallback
Elevation: Default

```
18:37:07.998  Received host key from the server. Algorithm: RSA/sha2-512, size: 3072 bits,
              SHA-256 fingerprint: O85OIxo9I45BBFc6n/x6OkyxLMhXZtkNU36qVfo4nVA.
18:37:07.998  First key exchange completed using Curve25519. Connection encryption and
              integrity: chacha20-poly1305, compression: none.
18:37:07.998  Attempting password authentication.
18:37:07.998  Authentication failed. Remaining authentication methods:
```

Copy the QS-Patch.tar file to the QuikStation via SFTP or SCP

1. In Bitvise, with an active session (created in the previous section), select **New SFTP Window**.
2. In the SFTP window that pops up, select the **Browse for folder** icon.
3. Navigate to the folder where you stored the QS-Patch.tar file, and click "OK".



Local path: C:\

Name	Size	Type	Date Modified
$Recycle Bin	0	File folder	11/1/2023 10:19 ...
$WinREAgent	0	File folder	11/1/2023 9:39 AM
Documents and Settings	0	File folder	11/1/2023 8:48 AM
Intel	0	File folder	11/6/2023 9:29 AM
PerfLogs	0	File folder	5/6/2022 10:24 PM
Program Files	0	File folder	11/6/2023 9:32 AM
Program Files (x86)	0	File folder	11/6/2023 1:43 PM
ProgramData	0	File folder	11/6/2023 9:32 AM
Recovery	0	File folder	11/6/2023 9:29 AM
System Volume Information	0	File folder	11/6/2023 12:34 ...
Users	0	File folder	11/6/2023 9:18 AM
Windows	0	File folder	11/6/2023 1:43 PM
Windows.old	0	File folder	11/6/2023 9:30 AM
DumpStack.log.tmp	12,288	TMP File	11/6/2023 9:30 AM
hiberfil.sys	13,637,09...	System file	11/6/2023 9:28 AM

Remote path: /home/vtx

Name	Size	Type	Date Modified

4. Select the QS-Patch.tar file from the **Local files** section on the Left and click the **Upload** icon.
5. When successful, you will see the uploaded file in the **Remote files** section on the Right.
   The default upload location on the QuikStation is the '**/home/vtx**' directory. This is the recommended location.

Extract Scripts from QS-Patch.tar file

1. Open a shell session on the QuikStation from the **New terminal console** Icon in Bitvise, or using the tool of your choice.
2. Verify the presence of the file by running this command: **ls**
   You should see QS-Patch.tar listed.
3. Extract the scripts from the file with this command: **tar -xvf QS-Patch.tar**. Then, issue **ls** again.
   You should see both **QS-security-patch.sh** and **webinterface.sh** listed.

Make the Scripts Executable

From the terminal, make both scripts executable with this command:
chmod +x QS-security-patch.sh webinterface.sh

You will not see any output when the command is run successfully.

Run the QS-security-patch.sh Script

1. From the terminal, execute the following command to run the script: **./QS-security-patch.sh**
   You should see the following output:
   ```
   Stopping Apache: OK
   Stopping ntpd: OK
   Status: Successfully completed
   ```

   ***NOTE:** If you attempt to run the script and you see "**Permission denied**", please see '**Make the Scripts Executable**' to resolve this error.*
2. Implement the changes by rebooting the QuikStation with this command: **reboot**

Enabling and Disabling the Web Management Interface

After applying the security patch, the Web Management Interface will be disabled. Should you need to enable it for configuration purposes, you will need to SSH into the QuikStation with the New Terminal Console tool from Bitvise, or the tools of your choice, and use the **webinterface.sh** script. It is important to remember that when you enable the Web Management Interface, it will remain active (and thus the system insecure) until the QuikStation loses power, is rebooted, or until you manually disable the Web Management Interface with the **webinterface.sh** script (which is recommended).

Enabling

Enable the Web Management Interface with this command:

./webinterface.sh enable

You will see the following output:

```
Web Interface has been started and will run until manually stopped or the
system is rebooted
```

Disabling

Keeping the Web Management Interface enabled leaves security vulnerabilities accessible. To disable the Web Management Interface, use this this command:

./webinterface.sh disable

You will see the following output:

```
Web Interface has been stopped and will remain stopped until manually started
```