Nikolaus-Groß-Straße 13,
44329 Dortmund
Germany

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

Nikolaus-Groß-Straße 13,
44329 Dortmund
Germany

- 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