Tandberg Data GmbH
Nikolaus-Groß-Straße 13,
44329 Dortmund
Germany

16.11.2023

Sehr geehrte QuikStation Kunden,

wir freuen uns, Ihnen einen neuen Satz Software-Patches für die RDX QuikStation 4- und QuikStation 8-Firmware anbieten zu können, welche die Sicherheit unseres Produkts erhöhen, indem sie eine Reihe von Problemen mit häufigen Sicherheitslücken und Gefährdungen (Common Vulnerabilities and Exposures, CVE) beheben. Die Patches können auf jeder QuikStation ab der Firmware Version 3.x.x.x installiert werden. Wir empfehlen, immer die neueste Firmware-Version zu verwenden (derzeit 3.2.1.2 zum Zeitpunkt der Veröffentlichung dieser Patches).

Bitte beachten Sie jedoch, dass zur Implementierung dieser wichtigen Sicherheitsupdates die Web-Benutzeroberfläche (UI) deaktiviert wird, solange keine aktiven Konfigurationen am System durchgeführt werden. Diese Maßnahme ist notwendig, um die Robustheit der Patches sicherzustellen und die Integrität des Systems aufrechtzuerhalten.

Wir verstehen, dass sich diese Änderung auf Ihre aktuelle Arbeitsweise mit Ihrer QuikStation auswirken kann, und danken Ihnen für Ihr Verständnis und Ihre Kooperation. Unser Team ist bestrebt, Ihnen ein sicheres und zuverlässiges Produkt zu bieten, und wir glauben, dass dieses Update ein wichtiger Schritt in Richtung dieses Ziels ist.

Ein Sicherheitsscan von RDX QuikStation 4 oder QuikStation 8 vor der Anwendung des Patches und der Deaktivierung der Webschnittstelle wird die folgenden Sicherheitsbedenken aufdecken:

- 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

Tandberg Data GmbH
Nikolaus-Groß-Straße 13,
44329 Dortmund
Germany

- 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

Nach der Anwendung des Patches und der Deaktivierung der Web-Benutzeroberfläche sehen Sie als einziges verbleibende offene Problem:

- ICMP timestamp response

Dieses Problem wird mit einer kommenden RDX QuikStation-Firmware-Version behoben werden.

Ihr Overland-Tandberg Team