ADVISORY

DATE

3 JUNE 2021

QNAP Q'center Virtual Appliance < 1.12.1014 Stored XSS

Summary

An unauthenticated attacker can inject JavaScript code on Q'center Virtual Appliance event log page.

Product Description (from vendor)

"Q'center now provides Q'center Virtual Appliance that allows you to deploy Q'center in virtual environments such as Microsoft Hyper-V or VMware ESXi, Fusion and Workstation. Using Q'center as a virtual appliance further increases its flexibility and connectivity for large environments, as you no longer need a local QNAP NAS to monitor other NAS and can use an existing central server to monitor every NAS unit." For more information visit https://www.qnap.com/solution/qcenter.

CVE(s)

- CVE-2021-28807

Details

Root Cause Analysis

The "Log" page in the "Q'center Event" tab shows all events that occurred on the Q'center server, including failed login attempts.

Among the information reported there is the name of the account that failed the login; because this parameter is controlled by the attacker and is not sanitized before being reflected in the page, an unauthenticated attacker could inject JavaScript code which will be executed whenever a privileged user navigates to the Q'center event section.

Proof of Concept

The complete PoC code can be found on this repo.

Impact

An unauthenticated attacker could hijack a privileged user session.

Remediation

Upgrade QNAP Q'Center to version 1.12.1014 or higher.

(Note: we didn't verify the patches.)

Disclosure Timeline

This report was subject to Shielder's disclosure policy.

- 23/01/2021: Vulnerability report is sent to QNAP
- 10/03/2021: QNAP acknowledges issue
- 11/03/2021: Shielder and QNAP agree on the impact of the vulnerability
- 03/06/2021: Shielder's advisory is made public

Credits

'zi0Black' of Shielder

This advisory was first published on https://www.shielder.com/advisories/qnap-qcenter-virtual-stored-xss/

INFO

Shielder S.r.l.

P.I. 11435310013

REA TO - 1213132

Registered Capital: 81.000,00 €

Via Palestro, 1/C
10064 Pinerolo (TO) Italy

CONTACTS

info@shielder.com

Landline: (+39) 0121 - 39 36 42

Commercial: (+39) 345 - 30 31 983

Technical: (+39) 393 - 16 66 814