ADVISORY

DATE

3 JUNE 2021

QNAP Q'center Post-Auth Remote Code Execution via QPKG

Summary

A privileged user can obtain remote code execution on Q'center through a manipulated QPKG installation package.

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

QNAP Q'center, a central management platform that enables to consolidate the management of multiple QNAP NAS, allows to upload and install QPKG packages.
"A QPKG file makes it easy for anyone to install and remove packages. It also gives a package maintainer almost total control on how the package is installed on the NAS." from QPKG Development Guidelines.

By opening a QPKG file with a hex editor it's immediately clear that the structure is composed by an initial script ending with `exit 10` followed by a tar.gz archive.
As the initial script seems to rule the archive extraction it is legitimate to think that it is extracted from the QPKG file and executed to extract what follows.

Q'center is available as a WMware appliance and it is possible to easily extract the Python code from its disk. The following script `/opt/qnap-cms/qnap-cms/python/hawkeye/patch.py` was extracted from it and it responbile to check a QKPG when it is uploaded to the Q'center.

```
237 def do_check():
238     [...]
239     try:
240     if os.path.isdir(tmp_folder_path):
241     shutil.rmtree(tmp_folder_path, True)
242     os.makedirs(tmp_folder_path)
243         with tarfile.open(path, 'r:gz') as (tar):  #[2]
244             tar.extractall(path=tmp_folder_path)   #[3]
245     if not os.path.isfile(patch_qpkg_path):
246     CMS_OPERATION.fire(user, cms_operation.PATCH_VERSION_ERROR,
247     source_ip)
248     return return_code
249     cmd = '/bin/sh %s'
250         utils.safe_call(cmd, patch_qpkg_path)      #[1]
251     os.remove(patch_qpkg_path)
252     [...]
```

The function extracts the update file (a tar.gz containing the QPKG one) at [2] and [3], then it executes the system command `/bin/sh /path/to/QPKG_file`.
As stated before the QPKG file could be interpreted as a shell script, so its content is executed on the Q'center instance, allowing to execute arbitrary commands on it.

Proof of Concept

The complete PoC code can be found on this repo.

Impact

A privilege attacker could obtain command execution on a Q'center instance.

Remediation

Our tests targeted the *QNAP Q'center Virtual Appliance*, and this vulnerability was identified in version 1.12.1014.
After reporting the vulnerability to QNAP they declared as **patched** the following QTS versions so we assume that the vulnerability affected both QTS and Q'center:

- QTS 4.3.3 : v.1.10.1004
- QTS 4.3.6 : v.1.10.1004
- QTS 4.5.3 : v.1.12.1012
- QuTS hero h4.5.2 : v.1.12.1012
- QuTS Cloud c4.5.4 : v.1.12.1012

(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-post-auth-remote-code-execution-via-qpkg/

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

SITEMAP

Home

Company

Services

Advisories

Blog

Careers

Contacts

Disclosure policy

Privacy policy