Security Advisory
QNAP QTS 4.3.3
Arbitrary File Retrieval Vulnerability

Created by Luca Carettoni
09/12/2017

Overview

This document provides the technical details of an arbitrary file retrieval vulnerability fixed by QNAP Systems affecting the latest QTS NAS Operating System.

On June 26th 2017, QNAP has released an update to address this issue. Information around the vulnerability was released in September 2017.

About Us

Doyensec is an independent security research and development company focused on vulnerability discovery and remediation. We work at the intersection of software development and offensive engineering to help companies craft secure code.

Research is one of our founding principles and we invest heavily in it. By discovering new vulnerabilities and attack techniques, we constantly improve our capabilities and contribute to secure the applications we all use.

QNAP QTS 4.3.3 Arbitrary File Retrieval Vulnerability	
Vendor	QNAP Systems, Inc.
Severity	High
Vulnerability Class	Injection Flaws
Component	QTS File Manager
Status	Fixed
CVE	Not Assigned
Credits	Luca Carettoni of Doyensec

Summary

A low-privileges user can escalate permissions to root abusing an arbitrary file retrieval vulnerability affecting QTS default File Manager. This issue leads to full system compromise.

Technical Description

Users with access to the “File Station” utility have the ability to “Compress Files”. This functionality can be abused to download arbitrary files from the NAS filesystem, resulting in system compromise.

It is possible to reproduce this issue by:

1. Selecting a random file from the file explorer
2. Clicking “Other Actions” and then “Compress”
3. Intercepting the HTTP request with a local proxy (eg. OWASP ZAP, Burp Proxy, …) and tampering the *compress_file* parameter as illustrated:

```
POST
/cgi-bin/filemanager/utilRequest.cgi?&func=compress&compress_file=/etc/config/shadow
HTTP/1.1

compress_name=luca&type=zip&level=normal&mode=1&path=/MyFolder&total=1&sid=hnr4q2oo
```

4. Downloading the newly created ZIP file (luca.zip). This archive will contain the remote */etc/shadow* file, which allows to perform offline bruteforcing of the admin password and any other local credentials.

All files and directories can be downloaded as well (e.g. system configurations) since the service runs as 'root'.

Remediation

QNAP has released an update (QTS 4.3.3.0229 build 20170624) to address this issue:

- https://www.qnap.com/en/releasenotes/?cat_choose=5

Disclosure Timeline

05/15/2017	Vulnerability disclosed to the vendor via online form
06/01/2017	Vendor's ack
06/12/2017	Vendor confirms the vulnerability and resolution in the next release
09/12/2017	Doyensec asks for updates on the vulnerability
09/12/2017	QNAP confirms that the vulnerability is fixed and points to the following release note:

QTS 4.3.3.0229 Build 20170624

(2017/06/26)

[Important Notes]
- For the status of QTS updates and maintenance for your NAS model, visit https://www.qnap.com/en/product/eol.php
- When QTS 4.3.x is installed on NAS models running on 64-bit Intel and AMD processors, some applications may not be supported. To check if installed apps on your NAS are compatible with QTS 4.3.x, download the QTS 64-bit compatibility tool and install it on your current QTS build. (https://download.qnap.com/QPKG/CF64_0.1-1114.qpkg.zip)
- QTS 4.3.x is the final available firmware update for the following models:
TS-112P, TS-212P, TS-212-E, HS-210, TS-112, TS-212, TS-121, TS-221, TS-421 TS-120, TS-220, TS-420, TS-420U, TS-421U TS-412, TS-412U, TS-419U, TS-419U , TS-419U II, TS-119P II, TS-219P II, TS-419P II, TS-119P , TS-219P , TS-419P , TS-119P, TS-219P, TS-419P, TS-119, TS-219, TS-419

[Enhancements]
- Improved the compatibility of the third and fourth drive bays on the TS-451A with high-capacity hard drives.

[Fixes]
- No disk I/O errors occur when an external storage device is selected as the destination for cloud-to-local sync jobs on Hybrid Backup Sync.
- Download Station does not lose connection when multiple download tasks are completed in a short period of time.
- The NAS can still join an Active Directory domain when SMB 1 is disabled on the Active Directory server.
- No connection issues occur when users access certain VPN servers via L2TP/IPSec or OpenVPN using QVPN.
- Domain users can access shared folders after installing a certain Qfix and then restart the NAS.
- The configuration of the DHCP server of the USB QuickAccess port does not affect the DHCP service in Container Station.
- Subtitles can be correctly displayed when users play .mp4 files on File Station.
- VJBOD disconnections do not cause Download Station to stop even when the download locations of download tasks are on the VJBOD volumes.
- Fixed multiple security vulnerabilities regarding input validation and access control.
- Temporary folders can be successfully deleted after users finish backing up files from the QNAP NAS to non-QNAP NAS devices via RTRR.
- Users can successfully delete a large number of LUNs using Cinder without causing Storage Manager interface to stop responding.
- The system does not erroneously display the message "update failed" when users enable or disable antivirus in Control Panel.