Sense of Security	Authorisation. Jason Edelstein
	Release date. 13 June 2012.

Sense of Security – Security Advisory – SOS-12-006.

QNAP Turbo NAS – Multiple Vulnerabilities.

13 June 2012.

QNAP Turbo NAS – Multiple Vulnerabilities - Security Advisory - SOS-12-006

Release Date.	13-Jun-2012
Last Update.	-
Vendor Notification Date.	12-Mar-2012
Product.	QNAP
Platform.	Turbo NAS (verified) and possibly others
Affected versions.	Firmware Version: 3.6.1 Build 0302T and prior
Severity Rating.	High
Impact.	Exposure of sensitive information Exposure of system information Privilege escalation System access
Attack Vector.	Remote with authentication
Solution Status.	Currently no software update; vendor has elected not to fix at this time
CVE reference.	CVE - not yet assigned

Details.

QNAP provide NAS technology solutions to consumers and enterprises. Multiple vulnerabilities have been identified in the web management interface.

1. Command Injection:

The QNAP Download Station (QDownload) is vulnerable to command injection as the application executes user-controllable data that is processed by a shell command interpreter.

The following resources, accessible post authentication are affected:

/cgi-bin/Qdownload/DS_RSS_Option.cgi [keyword parameter]

/cgi-bin/Qdownload/DS_RSS_Option.cgi [title parameter]

Commands are executed with the context of the admin user [uid=0(admin) gid=0(administrators] on the QNAP device.

Proof of Concept.

```
/cgi-bin/Qdownload/DS_RSS_Option.cgi?_dc=1331164660690&url=http%3A%2F%2Fgoogle.com&title=test&keyword=`touch%20%2ftesto%2etxt`&todo=add&sid=i9nonapr&ver=2.0
```

2. Cryptography:

The QNAP login page stores persistent cookies (including the administrator username and password) as base64 encoded strings inside the cookie parameter “nas_p”. These cookies are not protected with either the HTTPOnly or Secure flags allowing theft via one of the many cross-site scripting vulnerabilities which exist within the application (disclosed previously by another researcher, but never fixed).

Proof of Concept.

```
Cookie: qnap_admin_style=default; nas_save_u=1;
nas_u=bGFicw==; nas_address=10.1.1.2; nas_save_p=1; nas_p=
YWRtaW5UMG1iJTI0dDBuMw==; nas_tree_x=240; nas_tree_y=370
```

```
YWRtaW5UMG1iJTI0dDBuMw== decodes to admin123qweasd
```

Solution.

No vendor solution.

Discovered by.

Nadeem Salim and Phil Taylor from Sense of Security Labs.

About us.

Sense of Security is a leading provider of information security and risk management solutions. Our team has expert skills in assessment and assurance, strategy and architecture, and deployment through to ongoing management. We are Australia’s premier application penetration testing firm and trusted IT security advisor to many of the country's largest organisations.

Sense of Security Pty Ltd

Level 8, 66 King St
Sydney NSW 2000
AUSTRALIA

T: +61 (0)2 9290 4444
F: +61 (0)2 9290 4455
W: http://www.senseofsecurity.com.au
E: info@senseofsecurity.com.au
Twitter: @ITsecurityAU

The latest version of this advisory can be found at:

http://www.senseofsecurity.com.au/advisories/SOS-12-006.pdf

Other Sense of Security advisories can be found at:

http://www.senseofsecurity.com.au/research/it-security-advisories.php