Dear Synology users,

Synology® confirmed known security issues (reported as CVE-2013-6955 and CVE-2013-6987) which would cause compromise to file access authority in DSM. An updated DSM version resolving these issues has been released accordingly.

The followings are possible symptoms to appear on affected DiskStation and RackStation:

- **Exceptionally high CPU usage detected in Resource Monitor:**
  CPU resource occupied by processes such as dhcp.pid, minerd, synodns, PWNED, PWNEDb, PWNEDg, PWNEDm, or any processes with PWNED in their names
- **Appearance of non-Synology folder:**
  An automatically created shared folder with the name "startup", or a non-Synology folder appearing under the path of "/root/PWNED"
- **Redirection of the Web Station:**
  "Index.php" is redirected to an unexpected page
- **Appearance of non-Synology CGI program:**
  Files with meaningless names exist under the path of "/usr/syno/synoman"
- **Appearance of non-Synology script file:**
  Non-Synology script files, such as "S99p.sh", appear under the path of "/usr/syno/etc/rc.d"

If users identify any of above situation, they are strongly encouraged to do the following:

- For DiskStation or RackStation running on DSM 4.3, please follow the instruction here to REINSTALL DSM 4.3-3827.
- For DiskStation or RackStation running on DSM 4.0, it's recommended to REINSTALL DSM 4.0-2259 or onward from Synology Download Center.
- For DiskStation or RackStation running on DSM 4.1 or DSM 4.2, it's recommended to REINSTALL DSM 4.2-3243 or onward from Synology Download Center.

For other users who haven't encountered above symptoms, it is recommended to go to **DSM** > **Control Panel** > **DSM Update** page, update to versions above to protect DiskStation from malicious attacks.

Synology has taken immediate actions to fix vulnerability at the point of identifying malicious attacks. As proliferation of cybercrime and increasingly sophisticated malware evolves, Synology continues to casting resources mitigating threats and dedicates to providing the most reliable solutions for users. If users still notice their DiskStation behaving suspiciously after being upgraded to the latest DSM version, please contact security@synology.com.