

# A Security Audit of the Synology Disk Station Manager (DSM) v2.0-590

April 4th, 2008

Daniel Guido

[dguido@gmail.com](mailto:dguido@gmail.com)

Information Systems and Internet Security Laboratory at Polytechnic University

Report v0.8 DRAFT

# Table of Contents

0. Overview.....	3
Contents.....	3
Testing Methodology.....	3
Synopsis of Results.....	3
Table of Exposure.....	3
1. General Issues.....	4
All service daemons run with 'root' privileges.....	4
Service daemons do not turn off when disabled in the web interface.....	4
PostgreSQL and MySQL listen on a remote port unnecessarily.....	4
UPSd listens on a remote port unnecessarily.....	4
Inability to change administrative credentials.....	4
2. OpenSSH.....	4
SSH protocol version 1 enabled.....	4
3. Apache HTTP Server.....	5
Use of weak SSL ciphers and protocols.....	5
Deprecated SSL Protocol Usage.....	5
Debugging functions are enabled on the remote web server.....	5
Apache < 2.2.8 multiple vulnerabilities.....	5
Web applications are compiled binaries and run as root.....	6
4. PHP (File/Audio/Surveillance/Web Station).....	6
PHP < 5.2.5 multiple vulnerabilities.....	6
5. Samba (Windows File Sharing).....	6
NULL sessions are enabled on the remote host.....	6
Samba < 3.0.28 multiple vulnerabilities.....	6
Weak filesystem entitlement.....	7
6. rTorrent (Download Redirector).....	7
rTorrent < 0.7.9 potential vulnerabilities.....	7
7. Firefly Media Server (mt-daapd/iTunes Service).....	7
Firefly Media Server < 0.2.4.1 multiple vulnerabilities.....	7
8. OpenSSL.....	8
OpenSSL < 0.9.8f multiple vulnerabilities.....	8
9. Timeline.....	8
Vendor Contact.....	8
Version History.....	8

# 0. Overview

## Contents

This report documents security vulnerabilities found in the Synology Disk Station Manager (DSM) v2.0-590 firmware<sup>1</sup> distributed on all Synology NAS devices. The author of this document owns a CS407 and has modified it through the Synology-supported patches to enable Telnet and SSH. No other modifications were made.

## Testing Methodology

All testing was performed through Nmap<sup>2</sup>, Nessus<sup>3</sup>, and manual analysis of the filesystem over SSH. The raw reports of these scans are included in a zip with this report and can be easily replicated by re-running these tools on any Synology device. Only service daemons were tested for security vulnerabilities; no testing was done of any Synology-developed web applications.

## Synopsis of Results

This audit has discovered over 20 exploitable security vulnerabilities in Synology's DSM v2.0-590 firmware. These vulnerabilities are listed in a table below. All vulnerabilities found during the course of the audit were previously known and have been patched by upstream software developers, ie., no "0-day" vulnerabilities are released in this report. **Additionally, it should be noted that all remote code execution vulnerabilities result in complete, 'root' compromise of the device because all services are running with 'root' privileges.**

## Table of Exposure

Application	Port	Exposure	Section	Severity
All Services	All Ports	Unnecessary Privilege Levels Inability to change admin user	1	High Medium
OpenSSH	22	Encryption Bypass	2	Medium
Apache HTTPD OpenSSL	80, 443, 5000, 5001	Remote Code Execution Encryption Bypass Cross-Site Tracing XSS	3	High Low Low Medium
PHP	80, 443, 5000, 5001	Remote Code Execution Input Manipulation Information Leakage Denial of Service	4	High High High High
Samba	139, 445	Remote Code Execution Unauthorized Info Disclosure Weak filesystem entitlements	5	High High High
LPRng	515	Unauthorized Remote Access	1	Low
MySQL	3306	Unauthorized Remote Access	1	Low
UPSd	3493	Unauthorized Remote Access	1	Low
Firefly Media Server	3689	Remote Code Execution	7	High
PostgreSQL DB	5432	Unauthorized Remote Access x 2	1	Low
rTorrent	Client-side	Potential Code Execution	6	Low

1 [Synology Announces The New Synology Disk Station Manager 2.0 Software](#)

2 <http://nmap.org>

3 <http://nessus.org/nessus/>

# 1. General Issues

## All service daemons run with 'root' privileges

Problem: Remote code execution in any service will result in an attacker gaining full access to the machine.

Solution: Services should run under a restricted user which only has read/write access to the set of files that service requires.

Severity: **High**. The effect of this vulnerability is that remote code execution on any service results in root access to the Synology device and, therefore, access to all the users data among other things.

## Service daemons do not turn off when disabled in the web interface

Problem: The PostgreSQL and LPRng services remain in a running state even when they are disabled by the user.

Solution: Services should only start when needed through their init.d scripts.

Severity: Medium. There are performance-related benefits to correcting this behavior as well.

## PostgreSQL and MySQL listen on a remote port unnecessarily

Problem: PostgreSQL DB and MySQL DB are listening for remote connections. This opens up another attack vector for a potential intruder. Since all web applications which use these databases are contained locally, there is no reason for either of them to be listening for remote connections.

Solutions

- PostgreSQL: Comment out the "host" sections in /usr/syno/pgsql/etc/pg\_hba.conf
- MySQL: add 'skip-networking' to the end of my.cnf

Severity: Low-Medium.

## UPSD listens on a remote port unnecessarily

Problem: The UPSD service is unnecessarily remotely accessible by default. If such functionality is desired, there should be an option in the web interface to configure it.

Solution: Unknown, see references for documentation of the upsd package.

Severity: Low.

Reference: <http://www.networkupstools.org/>

## Inability to change administrative credentials

Problem: The username of the default administrative user ('admin') cannot be changed or disabled.

Solution: Allow new administrative accounts to be created and for the default account to be changed or disabled.

Severity: Medium.

# 2. OpenSSH

## SSH protocol version 1 enabled

Problem: SSH protocol version 1 is not cryptographically safe and is vulnerable to passive attacks which can be used to decrypt SSH traffic.

Solution: Change '#Protocol 2,1' in /etc/sshd\_config to 'Protocol 2'

Severity: Moderate.

Reference

- [OSVDB 2116](#) : PKCS 1 Version 1.5 Session Key Retrieval

## 3. Apache HTTP Server

### Use of weak SSL ciphers and protocols

Problem: An attacker may be able to passively capture traffic and decrypt its contents.

Solution: Configure Apache with 'SSLCipherSuite HIGH:MEDIUM' to disable support for weak SSL ciphers.

Severity: Low.

### Deprecated SSL Protocol Usage

Problem: The remote service accepts connections encrypted using SSL 2.0, which reportedly suffers from several cryptographic flaws and has been deprecated for several years. An attacker may be able to exploit these issues to conduct man-in-the-middle attacks or decrypt communications between the affected service and clients.

Solution: Configure Apache with 'SSLProtocol all -SSLv2' to disable support for deprecated SSL protocols.

Severity: Low.

Reference

- [Analysis of the SSL 3.0 protocol](#)

### Debugging functions are enabled on the remote web server

Problem: Apache supports the TRACE and TRACK methods, which are used to debug web server connections. These methods are subject to cross-site scripting attacks which an attacker can use to trick users into giving up website credentials.

Solution: Set 'TraceEnable off' in /usr/syno/apache/conf/httpd.conf.

Severity: Low.

References

- [Cross-Site Tracing \(XST\) Whitepaper](#)
- [US-CERT Vulnerability Note VU#867593](#) : Apache enables HTTP TRACE method by default
- [Apache HTTPD 2.2 Documentation, TraceEnable Directive](#)

### Apache < 2.2.8 multiple vulnerabilities

Problem: The web server may be affected by several security vulnerabilities fixed in recent versions of Apache httpd.

Solution: Upgrade Apache to at least version 2.2.8

Severity: Medium.

References

- [OSVDB 39003](#) : Apache HTTP Server HTTP Method Header Request Entity Too Large XSS
- [OSVDB 38636](#) : Apache HTTP Server mod\_autoindex.c P Variable UTF-7 Charset XSS
- [Apache httpd 2.2 vulnerabilities](#)

## Web applications are compiled binaries and run as root

Problem: All Synology-developed web applications are compiled CGI binaries (likely written in C or C++) and run with root privileges due to Apache running with root privileges. Programming errors in the request handling functions of the CGI binaries could allow remote code execution with root privileges on the device.

Solution: Reduce the privileges of the Apache HTTPD server and rewrite the web applications in an interpreted language.

Severity: **High**.

## 4. PHP (File/Audio/Surveillance/Web Station)

### PHP < 5.2.5 multiple vulnerabilities

Problem: The web server is affected by multiple, severe security vulnerabilities fixed in recent versions of PHP. Exploits for these vulnerabilities are publicly available and linked to below.

Solution: Upgrade PHP to at least version 5.2.5.

Severity: **High**. Any applications which use PHP are vulnerable to remote code execution because of security vulnerabilities in the PHP interpreter. This includes, but is not limited to, the administrative interface, the File Station, the Audio Station, the Surveillance Station, the Web Station, and the Photo Station.

References

- [OSVDB 32782](#) : PHP PECL Zip Extension zip:// URL Wrapper Overflow
- [OSVDB 32776](#) : PHP Session Extension php\_binary Heap Information Disclosure
- [OSVDB 32780](#) : PHP substr\_compare() Function Arbitrary Memory Disclosure
- [OSVDB 33962](#) : PHP ext/filter FILTER\_VALIDATE\_EMAIL Newline Injection
- [OSVDB 34730](#) : PHP substr\_count() Function Arbitrary Memory Disclosure
- [OSVDB 32769](#) : PHP Zend Engine Variable Destruction Deep Recursion Overflow
- [The Month of PHP Bugs](#)

## 5. Samba (Windows File Sharing)

### NULL sessions are enabled on the remote host

Problem: Unauthenticated users can gain access to a list of all users, a list of all shares, the password policy, and may be able to read/write to individual shares. Unauthenticated users are able to use this access to run exploits against Samba.

Solution: Set 'restrict anonymous = yes' in /usr/syno/etc/smb.conf to force users to authenticate before gaining access to Samba.

Severity: **High**.

Reference

- [Re: \[Samba\] IPC\\$ share accessible with arbitrary usernames/passwords](#)

### Samba < 3.0.28 multiple vulnerabilities

Problem: The Win/Mac file sharing service (Samba) is affected by multiple remote code execution vulnerabilities fixed in recent versions of Samba. These issues are remotely exploitable and are exacerbated by the presence of NULL sessions.

Solution: Upgrade Samba to at least version 3.0.28a.

Severity: **High**. In common Synology NAS deployments, the Samba service is accessible to the entire local network. In some situations, such as at a business or on a college campus, there are many users on the local network all with the ability to access the Samba service on Synology NAS devices. Successful exploitation of this vulnerability will give the attacker root access to the device.

References

- [Samba Security Releases](#)
- [OSVDB 34700](#) : Samba Unfiltered MS-RPC Calls Arbitrary Remote Command Execution
- [OSVDB 34732](#) : Samba SPOOLSS RPC Interface RFNPNEX Request Remote Overflow
- [OSVDB 27130](#) : Samba smdb Share Connection Saturation DoS

## Weak filesystem entitlement

Problem: All files written through Samba are 'chmod 777' and are accessible to anyone else using the same client machine. The effect of this vulnerability are that despite any user ownership, read-only, or no-access permissions a user sets on their files, other users on the same client can read and write to those restricted files.

Solution: Change the default permissions from 777 to something more restrictive, such as 770 or 700.

Severity: **High**. This issue critically affects all multi-user installations of Synology NAS devices.

Reference

- Synology forums: [Some general user/security considerations](#)

## 6. rTorrent (Download Redirector)

### rTorrent < 0.7.9 potential vulnerabilities

Problem: The download redirector service relies on an old version of rTorrent (0.3.6, released in early 2005). Later versions of rTorrent had security-related bugs fixed and version 0.3.6 may be vulnerable to remote code execution.

Solution: Upgrade rTorrent to at least version 0.7.9.

Severity: Low. Upgrading rTorrent will have additional performance-related benefits, as well as enable support for encrypted Bittorrent downloads.

Reference

- [rTorrent 0.4.1 Release Notes](#)

## 7. Firefly Media Server (mt-daapd/iTunes Service)

### Firefly Media Server < 0.2.4.1 multiple vulnerabilities

Problem: Firefly Media Server (mt-daapd) is affected by multiple remote code execution vulnerabilities.

Solution: Upgrade Firefly Media Server to at least version 0.2.4.1.

Severity: **High**. In common Synology NAS deployments, the iTunes service is accessible to the entire local network. In some situations, such as at a business or on a college campus, there are many users on the local network all with the ability to access the iTunes service on Synology NAS devices. Successful exploitation of this vulnerability will give the attacker full remote root access to the device.

References

- [Firefly Media Server Webserver.C Multiple Format String Vulnerabilities](#)

- [Firefly Media Server Multiple Null Pointer Dereference Vulnerabilities](#)

## 8. OpenSSL

### OpenSSL < 0.9.8f multiple vulnerabilities

Problem: The OpenSSL libraries in use by Synology are affected by multiple remote code execution vulnerabilities.

Solution: All applications using OpenSSL libraries must be recompiled with OpenSSL version 0.9.8f or higher.

Severity: **High**. Any application which processes data through OpenSSL libraries is vulnerable, including Apache and OpenSSH.

References

- [OSVDB 37895](#) : OpenSSL DTLS Implementation Unspecified Off-by-one Remote Code Execution
- [OSVDB 29262](#) : OpenSSL SSL\_get\_shared\_ciphers Function Unspecified Remote Overflow
- [OSVDB 29263](#) : OpenSSL SSLv2 get\_server\_hello Function Remote DoS
- [OSVDB 19919](#) : OpenSSL SSL\_OP\_ALL SSL 2.0 Verification Weakness
- [OSVDB 28549](#) : OpenSSL RSA Key PKCS #1 v1.5 Signature Forgery
- [OSVDB 29260](#) : OpenSSL Malformed ASN.1 Structure Resource Consumption DoS
- [OSVDB 29261](#) : OpenSSL Crafted Public Key CPU Consumption DoS

## 9. Timeline

### Vendor Contact

Initial vendor contact through tech support form – 03/17/2008

Vendor denial – 03/18/2008

Vendor provided with v0.3 of report – 03/18/2008

Vendor acknowledgment – 03/18/2008

Vendor sends back initial findings – 03/22/2008

Vendor provided with v0.6 of report – 03/22/2008

Vendor provided with v0.7 of report - 03/28/2008

### Version History

v0.1 – 03/17/2008 – Initial document

v0.2 – 03/18/2008 – Fixed formatting

v0.3 – 03/18/2008 – Added severity levels

v0.4 – 03/19/2008 – Fixed formatting

v0.5 – 03/20/2008 – Added exposure table

v0.6 – 03/21/2008 – Fixed references

v0.7 – 03/29/2008 – Added OpenSSL, removed phpinfo, updated Apache references

v0.8 – 04/04/2008 – Added inability to change admin account, cgi binaries in Apache, public release