

DataDirectTM

NETWORKS



SFATM OS

OpenSSL Security Issues Addressed

Technical Support Bulletin

Revision A0
5 March 2015

1.0 Issue Description

1.1 OpenSSL Security Vulnerabilities

Security vulnerabilities in the OpenSSL encryption protocol have been resolved in SFA OS version 2.2.1.0. Among the resolved issues are those known as the “CRIME”, “Lucky 13” “CCS Injection”, and “SQUEEZ” vulnerabilities. These vulnerabilities allowed attackers to crack private keys, recover plaintext message content, hijack an authenticated session, inject arbitrary code, or cause denial of service.

1.2 Affected Systems

All SFA OS versions earlier than 2.2.1.0 are affected by these vulnerabilities. Affected storage platforms include the S2A6620, SFA7700, SFA10K, SFA10KE, SFA12K, SFA12KE, SFA12KX, and SFA12KXE.

2.0 SFA OS Resolution

SFA OS 2.2.1.0 ships with OpenSSL version 0.9.8o-4squeeze16. This new version of OpenSSL resolves the following security issues:

- CVE-2011-1945
- CVE-2011-3210
- CVE-2011-4108
- CVE-2011-4109
- CVE-2011-4576
- CVE-2011-4577
- CVE-2011-4619
- CVE-2012-0050
- CVE-2012-0884
- CVE-2012-1165
- CVE-2012-2110
- CVE-2012-2131
- CVE-2012-2333
- CVE-2012-4929
- CVE-2013-0166
- CVE-2013-0169
- CVE-2014-0076

- CVE-2014-0195
- CVE-2014-0221
- CVE-2014-0224
- CVE-2014-3470

3.0 Contacting DDN Technical Support

Feel free to contact DDN Technical Support with questions or requests for assistance. Support can be reached at any time by phone, by email, or on the web.

Telephone

DDN Support Worldwide Directory <http://www.ddn.com/support/contact-support>

Email

Support Email support@ddn.com

Web

Support Portal <https://portal.ddnsupport.com>
Portal Assistance webportal.support@ddn.com

Bulletins

Support Bulletins <http://www.ddn.com/support/technical-support-bulletins>
Bulletin Subscription Requests support-tsb@ddn.com