DDN STORAGE

TECHNICAL SUPPORT BULLETIN

DDN TECHNICAL SUPPORT | SPT-TSB-0054 (A3) | 14 JULY 2016

SFA OS™

Insecure Static Keys and Insecure Update Imaging Process

Issue Summary

DDN has been made aware of two security vulnerabilities in SFA OS that can allow unauthorized attackers to access the SFA controllers or execute code on the system as root. These vulnerabilities are exposed only if customers install the equipment on an unsecured network, contrary to DDN's recommended installation practices.

Because the security firm that published these vulnerabilities is not a registered CVE Numbering Authority, reports on these vulnerabilities have not been filed with the National Institute of Standards and Technology (NIST) and no CVE reference number has been assigned to them in the national Common Vulnerabilities and Exposures database. Consequently, we refer to them here by the security firm's own numbers, MWR-2016-0001 and MWR-2016-0002.

DDN takes all security vulnerabilities seriously and responds to them as defined in our published Security Policy.

Insecure Update Imaging Process (MWR-2016-0001)

The mechanism used for updating firmware on SFA controllers is insecure, allowing escalation of access privileges to root. An adversary could exploit this vulnerability to execute arbitrary code as root on the controller.

Affected Systems

This vulnerability was found to be common across all SFA products and SFA OS versions tested.

Workarounds

The following options are available as workarounds until a patch is released:

- ***Storage arrays and management console devices should be connected to a private network with restricted access***. Network isolation protects the equipment from attack. This is DDN's recommendation for all storage array installations.

- ***Only DDN-approved personnel should perform firmware upgrades on SFA equipment***. Customers with onsite support contracts can take advantage of this service at no charge.

- ***Customers who install their own firmware should procure upgrade images directly and exclusively from DDN Support***. Do not trust firmware hosted on a third-party server unless directed by DDN Support to do so.

Resolution

DDN is changing its code signing process to use public key cryptography, thereby ensuring that all SFA firmware originates from a trusted source. This enhancement will be available in a future release of SFA OS. Release is expected in October 2016.

Static Keys in SFA OS User Accounts (MWR-2016-0002)

Description and Impact

SFA storage controllers ship with a set of static entries in the `authorized_keys` file of several SFA OS user accounts. The corresponding private keys are disclosed in firmware updates that are publicly available. An adversary can make use of these keys in order to gain access to the SFA controller, even if the default passwords have been changed.

Affected Systems

This vulnerability was found to be common across all SFA products and SFA OS versions tested.

Workarounds

The following options are available as workarounds until a patch is released:

- ***Storage arrays and management console devices should be connected to a private network with restricted access***. Network isolation protects the equipment from attack. This is DDN's recommendation for all storage array installations.

- ***On SFA OS 3.0.0 and later, implement the Role Based Access Control (RBAC) feature of SFA OS.*** Once RBAC is in place, delete the pre-installed user accounts and the pre-installed SSH keys from the `authorized_keys` files. If assistance is needed with this procedure, please call DDN Support.

- ***On SFA OS 2.3.1.x and earlier, disable SSH access to the controllers*** until a patch becomes available. Note that this option should be considered a last resort, since access to the CLUI will be disabled while SSH is disabled, and SCP will be disabled as well. If you choose this option, please contact DDN Support for assistance with disabling and re-enabling SSH.

Resolution

DDN will remove the static keys from the SFA OS firmware in a future release of SFA OS. Release is expected in October 2016.

Contacting DDN Technical Support

Please contact DDN Technical Support at any time if you have questions or require assistance. Support can be reached by phone, by email, or on the web as listed below.

Web	
DDN Community Support Portal	https://community.ddn.com/login
Portal Assistance	webportal.support@ddn.com
Telephone	
DDN Support Worldwide Directory	http://www.ddn.com/support/contact-support
Email	
Support Email	support@ddn.com
Bulletins	
Support Bulletins	http://www.ddn.com/support/technical-support-bulletins
End-of-Life Notices	http://www.ddn.com/support/end-of-life-notices
Bulletin Subscription Requests	support-tsb@ddn.com