MWR LABS Security Advisory

DDN Default SSH Keys

2016-06-15

Software	SFAOS, all versions: SFA6620, SFA7700, SFA10K, SFA12K, SFA14K
Affected Versions	All current versions are believed to be affected
CVE Reference	No CVE assigned (MWR Ref: MWR-2016-0002)
Author	John Fitzpatrick
Severity	High
Vendor	DataDirect Networks (DDN)
Vendor Response	Uncooperative

Description

DDN controllers ship with a set of static entries within the authorized_keys file of several of the user accounts. The corresponding private keys can be obtained from publicly available sources.

Impact

An adversary can make use of these keys in order to gain access to the DDN controller even if the default passwords have been changed.

Cause

Insecure design and device hardening.

Interim Workaround

MWR strongly recommend restricting access to all DDN management interfaces via the use of ACLs until DDN provide an appropriate resolution to this issue.

Solution

DDN have not provided a solution to this and have indicated that they may resolve it towards the end of the second half of 2016. Exploitation of this issue combined with MWR-2016-0001 (DDN Insecure Imaging Process) can provide the access required in order to resolve this but may affect any warranty/support contract covering the devices.

A solution to this issue will require a firmware update from DDN which removes these keys on deployment of new firmware.

Further Information

DDN controllers run a Debian derived Linux distribution which has a number of different users. Some of these users are configured with an authorized_keys entry permitting them to log in via SSH using the corresponding private key. The authorized_keys entries were found to be common across all DDN devices and versions tested meaning exposure of the corresponding private keys would provide an adversary access to all DDN devices.

The corresponding private key was found to also be included within the firmware distributed for DDN controllers. DDN firmware is available for download by any DDN customer, although with some searching can also be found publicly too.

The following user accounts on the DDN controllers were found to permit authentication using known keys. The respective MD5sums are shown below:

```
diag:
/home/diag/.ssh$ md5sum *
e5138c922279b8d194896bacefc31992  authorized_keys
d2a101dc1f8dd610c146735d71d7e77a  id_rsa
```

```
stats:
/home/stats/.ssh$ md5sum *
7c3c7a068e07ed28a84eba1d3b4812a1  authorized_keys
ffe5fdd80332ed5170851b3d8cdf6f30  id_rsa
```

```
user:
/home/user/.ssh$ md5sum *
7c3c7a068e07ed28a84eba1d3b4812a1  authorized_keys
ffe5fdd80332ed5170851b3d8cdf6f30  id_rsa
```

```
ddn:
/ddn/.ssh$ md5sum *
1076f91f58db9040d87fe29b863ad5b7  authorized_keys
202a962bac24c892c1248dff050d413c  id_rsa
```

Anyone in possession of the respective private keys would be in a position to authenticate via SSH as any one of the users listed above.

The root user does not have any authorized_keys entries, additionally the default SSH configuration does not permit root to log in via SSH. The firmware user also has no authorized_keys entries.

When combined with the vulnerability described in “DDN Insecure Update Process – MWR-2016-0001” it is possible to gain full root access to a DDN controller.

This advisory will be updated appropriately should DDN choose to provide a solution to this security issue.

Timeline

Date	Summary
2016-03-09	Initial contact made with DDN
2016-03-14	Conference call with DDN engineers
2016-03-15	Full vulnerability details provided to DDN
2016-05-16	Advisory released for limited disclosure
2016-06-15	Advisory released

(Thanks to those who were key in identifying this vulnerability)