MWR LABS Security Advisory

DDN Insecure Update Process

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-2016-0001)
Author	John Fitzpatrick
Severity	High
Vendor	DataDirect Networks (DDN)
Vendor Response	Uncooperative

Description

The mechanism used for updating firmware on DDN controllers is insecure allowing for privilege escalation to root.

Impact

Exploitation of this issue can allow for code execution as root allowing an adversary to gain full access to the DDN controller.

Cause

This is caused by an insecure firmware update mechanism which does not validate the legitimacy of the firmware being uploaded.

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. In addition it should be ensured that appropriate mitigating controls are implemented for the accompanying advisory “DDN Default SSH Keys - MWR-2016-0002” and that default user account passwords are changed.

Solution

There is no vendor supplied solution to this vulnerability. When DDN have resolved this vulnerability DDN users should apply the appropriate fixes.

It is recommended that DDN implement a signing mechanism that validates that firmware is from a trusted source before attempting to deploy it. Making use of public key cryptography in order to sign firmware would be a suitable approach if correctly implemented. DDN have, however, chosen not to comment on their preferred resolution or its progress but have indicated that they may resolve this issue towards the end of 2016.

Further Information

DDN firmware is provided as a .tar file. Within this archive is another archive containing the contents of the filesystem which, when an update is run, is extracted and deployed to disk. A number of shell scripts also execute during the update process and these are executed as root. Therefore, by either manipulating the shell scripts or by modifying the filesystem contents within the archive, it is possible perform activities which would provide full root access to the DDN device.

There is a signing mechanism in place; however, this is focused on ensuring files are not corrupt rather than ensuring that files are from a legitimate source. Within janus.md5 is a list of MD5 checksums for all files within the archive. These entries can simply be replaced with new MD5s as appropriate.

In order to perform an update, it is necessary to have access to accounts on the DDN controller. Our testing was performed via SSH using the firmware account to drop the firmware. This account has a very guessable password set by default. The ddn user account was then used in order to load the new config/firmware via the appropriate menu options. The ddn user also has a default password set, but this is much less guessable. However, even if the default passwords have been changed it will be possible to use the default SSH keys described in MWR-2016-0002 (DDN Default SSH Keys) in order to gain the required level of access in order to deploy the new firmware.

Ironically, successful exploitation of this insecure update mechanism allows DDN users to remove the default SSH keys and secure their devices. Whether this would impact support contracts or warranties with DDN or other suppliers is unknown.

This advisory will be updated should DDN choose to provide an appropriate 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)