MWR LABS

Security Advisory

IBM GPFS / Spectrum Scale Command Injection

2016-06-07

Software	GPFS / Spectrum Scale
Affected Versions	IBM Spectrum Scale V4.2.0.0 thru V4.2.0.2 IBM Spectrum Scale V4.1.1.0 thru V4.1.1.6 IBM GPFS V4.1.0.0 thru V4.1.0.8 IBM GPFS V3.5.0.0 thru V3.5.0.30 All older IBM GPFS versions no longer supported
CVE Reference	CVE-2016-0392
Author	John Fitzpatrick
Severity	High
Vendor	IBM
Vendor Response	Fixes provided

Description

IBM's General Parallel File System (GPFS), now known as Spectrum Scale, is affected by a vulnerability that allows an adversary on any system which mounts GPFS to inject commands which are later executed as root.

Impact

Exploitation of this vulnerability allows any user of a system with a GPFS filesystem mounted to execute commands as root across the GPFS cluster.

Cause

This is caused by a failure to safely handle arguments supplied to a number of setuid binaries.

Interim Workaround

IBM have provided patches in order to resolve this issue. It is recommended that these patches (described in the 'Solution' section below) are applied. However, if this is not possible some workarounds may also be applied:

Remove the setuid from the files in the /usr/lpp/mmfs/bin directory. These can be identified by running

```
ls -l /usr/lpp/mmfs/bin | grep r-s
```

Reset the setuid bit for each such file by issuing this command on each file

```
chmod u-s file
```

Once the workaround is applied, a number of commands may no longer work when not invoked by unprivileged users, including:

```
mmchfileset
mmcrsnapshot
mmdelsnapshot
mmdf
mmedquota
mmgetacl
mmlsdisk
mmlsfileset
mmlsfs
mmlsmgr
mmlspolicy
mmlspool
mmlsquota
mmlssnapshot
mmputacl
mmsnapdir
```

(These workarounds are taken from the IBM supplied advisory which can be found at: http://www-01.ibm.com/support/docview.wss?uid=isg3T1023763)

If the workarounds would not affect the usability of GPFS within your environment, then MWR recommend applying these workarounds in addition to the IBM supplied patches detailed below.

Solution

IBM have provided fixes for this issue; however, MWR have not tested the effectiveness of these patches:

- For IBM Spectrum Scale V4.2.0.0 thru V4.2.0.2, apply IBM Spectrum Scale V4.2.0.3 available from Fix Central at:

  http://www-933.ibm.com/support/fixcentral/swg/selectFixes?parent=Software%2Bdefined%2Bstorage&product=ibm/StorageSoftware/IBM+Spectrum+Scale&release=4.2.0&platform=All&function=all

- For IBM Spectrum Scale V4.1.1.0 thru 4.1.1.6 and IBM GPFS V4.1.0.0 thru V4.1.0.8, apply V4.1.1.7 at:

http://www-933.ibm.com/support/fixcentral/swg/selectFixes?parent=Software%2Bdefined%2Bstorage&product=ibm/StorageSoftware/IBM+Spectrum+Scale&release=4.1.1&platform=All&function=all

- For IBM GPFS V3.5.0.0 thru V3.5.0.30, apply V3.5.0.31 at:

  http://www-933.ibm.com/support/fixcentral/swg/selectFixes?parent=Cluster%2Bsoftware&product=ibm/power/IBM+General+Parallel+File+System&release=3.5.0&platform=All&function=all

For older versions of IBM GPFS, if you have an extended service contract, please contact IBM Service.

(These solutions are taken from the IBM supplied advisory which can be found at: http://www-01.ibm.com/support/docview.wss?uid=isg3T1023763)

Further Information

The IBM advisory relating to this issue can be found at the following location: *http://www-01.ibm.com/support/docview.wss?uid=isg3T1023763*

This issue is closely related to a format string issue in GPFS (CVE-2015-0197) found by Florian Grunwo and Felix Wilhelm of ERNW: *http://www-01.ibm.com/support/docview.wss?uid=isg3T1022062*

Further technical information may be released at a later date when users have had a chance to resolve this issue.

Detailed Timeline

Date	Summary
2016-04-02	Issue reported to IBM PSIRT
2016-05-31	Patch and vendor advisory released
2016-06-07	MWR advisory released