MWR LABS

Security Advisory

IBM Spectrum LSF Privilege Escalation

16th March 2018

Software	IBM Spectrum LSF
Affected Versions	IBM Spectrum LSF 8.3, 9.1.1, 9.1.2, 9.1.3, 10.1, 10.1.0.1
CVE Reference	CVE-2017-1205
Author	John Fitzpatrick
Severity	CVSS 9.3
Vendor	IBM
Vendor Response	Fixes provided

Description:

A vulnerability was identified within IBM Spectrum LSF which made it was possible to impersonate other users when submitting jobs for execution. Additionally, it was found to be possible to impersonate and execute jobs as root, even where root job submission is disabled.

Impact:

This vulnerability allows for arbitrary code execution as any user of the LSF cluster, including as root.

Exploitation should only be possible from hosts listed within lsf.cluster.cluster_name, which typically will include all hosts that form part of the cluster. However, some cluster use cases may be more open using ranges or wildcards; thus, exposure may extend beyond those with cluster access.

Cause:

This issue arises as a result of series of security oversights within LSF's authentication mechanism:

1. A hardcoded key embedded within the eauth binary, which is shared across all LSF installations, makes it possible for anyone with a copy of eauth to generate authentication tokens for any user in a default installation.

2. Even where eauth is configured to use an external key (non-default), overriding getuid() results in the ability to generate authentication tokens as other users.
3. On receiving job requests, LSF performs authentication and authorisation checks against the authentication token, but then proceeds to submit the job for execution against a UID contained elsewhere in the message, which is not validated. It is this behaviour that circumvents controls that prevent root job execution.

Interim Workaround:

Configure eauth to use an external key and set the setuid bit on the eauth binary in order to prevent users from runtime patching the eauth binary.

Details on how to configure eauth to use an external key can be found here::
https://www.ibm.com/support/knowledgecenter/en/SSWRJV_10.1.0/lsf_admin/ext_auth_kerb_lsf_about.html

Eauth can be configured with the setuid bit set in the following manner:

```
# chmod 4755 eauth
```

The guidance above does not resolve LSF's failure to validate the UID under which the job is run. However, unless an authentication token is disclosed, or another vulnerabilities exist, it should not be possible for a user to exploit this weakness without already having administrative rights within the cluster.

Solution:

IBM has provided some updates to address these issues, which can be found within their bulletin here:

http://www-01.ibm.com/support/docview.wss?uid=isg3T1025091

These fixes do not configure LSF to utilise an external key which should be done by creating a key and setting LSF_EAUTH_KEY within lsf.sudoers:
https://www.ibm.com/support/knowledgecenter/en/SSETD4_9.1.2/lsf_config_ref/lsf.sudoers.5.html

At the time the updates were provided, they failed to set the setuid bit on eauth and so, failed to actually resolve a core part of the issue. However, the setuid bit is set on eauth by default in the most recent installations and can be set manually. It should be ensured that your eauth uses an external key, is root owned and has the setuid bit set (chmod 4755).

If eauth has been configured to use an external key, but with no setuid bit set, then a new key should be generated.

Detailed Timeline

Date	Summary
2017-03-28	Issue reported to IBM PSIRT
2017-04-07	IBM report issue resolved, patches and security bulletin released
2017-04-12	Additional technical detail on fixes provided to MWR by IBM PSIRT
2018-03-16	Advisory published by MWR

Further Information

Further details on eauth and how it works can be found here:
https://www.ibm.com/support/knowledgecenter/en/SSWRJV_10.1.0/lsf_admin/ext_auth_kerb_lsf_about.html

Information on setting up eauth to use an external key:

https://www.ibm.com/support/knowledgecenter/en/SSETD4_9.1.2/lsf_config_ref/lsf.sudoers.5.html

IBM's security bulletin relating to this issue can be found here:

http://www-01.ibm.com/support/docview.wss?uid=isg3T1025091