SGI Tempo System Database Password Exposure

2nd December 2014

Software:	SGI Tempo (SGI ICE-X Supercomputers)
Affected Versions:	Unknown
CVE Reference:	CVE-2014-7301
Author:	John Fitzpatrick, MWR Labs (http://labs.mwrinfosecurity.com/)
Severity:	Medium Risk
Vendor:	Silicon Graphics International Corp (SGI)
Vendor Response:	Uncooperative

Description:

It is possible for users to gain read+write access to the Tempo system (configuration) database on SGI ICE-X supercomputers due to insecurely set file permissions on the /etc/odapw file.

Impact:

SGI describe the system database as “critical to the operation of your SGI ICE X system”. It is believed that this level of access could be used to cause significant disruption to the operation of the supercomputer. However, this has not been fully explored.

Cause:

Insecure (world readable) file permissions are set on the /etc/odapw file which contains the password for this database.

Solution:

SGI have chosen not to issue a fix. However, a workaround is trivial: Modify file permissions of the /etc/odapw file:

```
# chmod 600 /etc/odapw
```

Technical Details

SGI Tempo cluster management software, deployed on SGI ICE supercomputers, makes use of a system database (SDB, sometimes referred to as the Oscar database). This database (MySQL) contains system configuration information required for the operation of the cluster which, if altered, could cause severe disruption to the systems operation. In addition some information would be considered sensitive, particularly in more recent Tempo versions that have been found to store root password hashes as attributes within this database.

If root password hashes are held within the database they will be displayed as the result of running the following command:

```
# cattr list passwd_root
```

By default an anonymous account is available to query the SDB with read only permissions. An article on the SGI Supportfolio describes this issue and how to disable anonymous access:

https://support.sgi.com/kb_request/solution/display?KB_NODEUUID=62590135-708d-47d7-934e-b3fac09b7603&MODE=multiple *(Registration required)*

Disabling anonymous access will prevent non root users from running the c* commands (e.g. cattr, cnodes, etc.). Whilst providing read-only access does present its risks, the risk posed by providing read+write access is far more substantial as it can also be utilised to alter the system configuration and cause the system to fail to operate.

The default username for the database is “oscar”. The password for this is held in the /etc/odapw file which is present on service nodes and readable by all users of the system. The password follows a common structure shown below:

```
regexp: oscar(\.[0-9]{3}){4}

example: oscar.324.519.262.397
```

The following MySQL command will establish a connection to the database and prompt for the password within the /etc/odapw file:

```
$ mysql -u oscar -h admin -p
```

Workaround

MWR recommend altering the permissions of the /etc/odapw file to prevent non root users from reading the password. This will prevent non root users from being able to make use of the c* commands:

```
# chmod 600 /etc/odapw
```

SGI have chosen not to co-operate with MWR in the co-ordinated disclosure of this and other SGI related security issues. MWR are therefore unable to provide specific version information and other details. Whilst every effort has been made to ensure the accuracy and usefulness of this advisory it is recommended that SGI are contacted directly if further information is required.

Detailed Timeline

Date:	Summary:
2014-02-11	Contact with SGI established
2014-02-20	Full vulnerability details provided to SGI
2014-04-14	Vulnerabilities acknowledged and response provided
2014-05-23	Update requested by MWR (not provided)
2014-07-23	Update requested by MWR (not provided)
2014-11-20	Contact with SGI re-attempted
2014-12-02	Advisory published