

The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE

Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.

<http://www.us-cert.gov/tlp/>

DATE(S) ISSUED:

11/06/2015

SUBJECT:

Vulnerability in Cisco Mobility Services Engine Could Allow Unauthorized Access and Lead to Information Disclosure

OVERVIEW:

A vulnerability has been discovered in Cisco Mobility Services Engine, which could allow for unauthorized access, and lead to information disclosure. This vulnerability could allow an unauthenticated, remote user to log in with the default oracle account. This account does not have full administrator privileges. However, this access could lead to unintended information disclosure.

THREAT INTELLIGENCE:

There are currently no reports of this vulnerability being exploited in the wild.

SYSTEMS AFFECTED:

- Cisco Mobility Services Engine versions 8.0.120.7 and earlier

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: N/A

TECHNICAL SUMMARY:

A static password was assigned to the default oracle account on Cisco Mobility Services Engine (MSE). This account is a reserved account used for internal Mobility Services Engine tasks. This account does not have full administrative privileges, however access to it could lead to disclosure of sensitive internal information. MSE does not perform SSH logins with this account, and it should not be used in this manner. Signs of compromise can be determined by running the following command from the device.

```
mse> grep "user oracle" /var/log/secure* | grep "sshd:session"
```

This vulnerability has been fixed in all versions after Cisco MSE Static Credential Vulnerability 8.0.120.7. The following work around may also be applied to mitigate against this vulnerability.

1. Log in to the MSE as user *root*.
2. Edit the file `/etc/ssh/sshd_config` via a text editor.
3. Navigate to the bottom of the file and add the following line:
`DenyUsers oracle`
Note: This change only takes effect after the SSH service is restarted.
4. Save the updated `/etc/ssh/sshd_config` file.
5. Restart the SSH service with the **service sshd restart** command.
6. To verify that the workaround is properly configured, attempt an SSH login to the MSE as the *oracle* user.
 - a. This login attempt should fail with the error **<Permission Denied>**.
`ssh -l oracle <x.x.x.x>`
 - b. Try an SSH login to the MSE as the *root* user. This login attempt should succeed.
`ssh -l root <x.x.x.x>`

RECOMMENDATIONS:

The following actions should be taken:

- Apply patches or work around to vulnerable systems after appropriate testing.
- Administrators are advised to allow only trusted users to have network access.
- Administrators may consider using IP-based access control lists (ACLs) to allow only trusted systems to access the affected systems.
- Administrators are advised to monitor affected systems.

REFERENCES:

Cisco:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20151104-mse-cred>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6316>

TLP: WHITE

Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.

<http://www.us-cert.gov/tlp/>