

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 ISSUED:

07/02/2015

SUBJECT:

Vulnerability in Cisco Unified Communications Domain Manager Could Allow Elevation of Privilege

OVERVIEW:

A vulnerability has been discovered in Cisco's Unified Communications Domain Manager Platform Software which could allow for an elevation of privilege. This vulnerability could allow an unauthenticated, remote attacker to login with the privileges of the root user and take full control of the affected system. Failed attacks may cause a Denial of Service condition within the targeted delivery method. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

THREAT INTELLIGENCE:

There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:

- Cisco Unified Communications Domain Manager Platform prior to version 4.4.5
- Cisco Unified Communications Domain Manager versions 8.x

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 vulnerability has been discovered in Cisco's Unified Communications Domain Manager Platform which could allow for an elevation of privilege. The vulnerability occurs because a privileged account has a default and static password. This account is created at installation and cannot be changed or deleted without impacting the functionality of the system. An attacker could exploit this vulnerability by remotely connecting to the affected system via SSH using this account.

An unauthenticated, remote attacker could exploit this vulnerability to gain unauthorized access to an affected system with the privileges of the root user. A successful exploit could result in a complete system compromise. Failed attacks may cause a Denial of Service condition within the targeted delivery method. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

RECOMMENDATIONS:

The following actions should be taken:

- Apply patches 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/viewAlert.x?alertId=39512>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4196>

TLP: WHITE

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

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