

*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:**

09/21/2016

**SUBJECT:**

Vulnerabilities in Cisco Cloud Services Platform Could Allow for Arbitrary Command Execution

**OVERVIEW:**

Multiple vulnerabilities have been discovered in Cisco Cloud Services Platform that can result in arbitrary command execution and remote command injection. Cisco Cloud Services Platform 2100 is a turn-key, open x86 Linux Kernel-based Virtual Machine software and hardware platform for data center network functions virtualization. Attackers can exploit these issues to execute arbitrary commands on the host operating system with the privileges of root. Successful exploitation could allow an unauthenticated user to take control of the affected system and perform unauthorized actions.

**THREAT INTELLIGENCE:**

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

**SYSTEM AFFECTED:**

- Cisco Cloud Services Platform 2100 version 2.0 and prior

**RISK:**

**Government:**

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

**Businesses:**

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

**Home users: N/A**

**TECHNICAL SUMMARY:**

Cisco Cloud Services Platform 2100 is prone to two vulnerabilities that could allow for arbitrary code execution. These vulnerabilities are as follows:

- A vulnerability due to insufficient sanitization of specific values received as part of a user-supplied HTTP request. An attacker could exploit this vulnerability by sending a malicious 'dnslookup' request to the affected system. An exploit could allow the attacker to execute arbitrary code with the privileges of the user.

- A vulnerability due to insufficient sanitization of user-supplied input. An attacker could exploit this vulnerability by authenticating to the affected system with administrative privileges and inserting arbitrary commands. An exploit could allow the attacker to execute arbitrary commands on the host operating system with the privileges of root.

Successful exploitation could allow remote attackers to perform unauthorized actions.

#### **RECOMMENDATIONS:**

The following actions should be taken:

- Install updates once released by Cisco after appropriate testing.
- Verify no unauthorized system modifications have occurred on system before applying patch.
- Monitor intrusion detection systems for any signs of anomalous activity.
- Unless required, limit external network access to affected products.

#### **REFERENCES:**

##### **Cisco:**

<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160921-csp2100-1>

<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160921-csp2100-2>

##### **CVE:**

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6373>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6374>

#### **TLP: WHITE**

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

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