

*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.*

**DATE(S) ISSUED:**

05/01/2014

**SUBJECT:**

Multiple Vulnerabilities in Cisco Telepresence TC and TE Software

**EXECUTIVE SUMMARY:**

Multiple vulnerabilities have been discovered in Cisco Telepresence TC and TE software which is used by Cisco Telepresence hardware. The exploitation of these vulnerabilities could allow a remote attacker to gain unauthorized access to the device and network, or to elevate privileges and gain administrative access to the affected system, or cause denial of service conditions.

**THREAT INTELLIGENCE**

Currently we are not aware of any malicious exploitation of these vulnerabilities in the wild.

**SYSTEMS AFFECTED:**

Cisco Telepresence Systems:

- Cisco Telepresence Integrator C Series
- Cisco Telepresence MX Series
- Cisco Telepresence Profiles Series
- Cisco Telepresence Quick Set Series
- Cisco Telepresence System EX Series
- Cisco Telepresence System T Series
- Cisco Telepresence VX Clinical Assistant

## **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: Low**

## **TECHNICAL SUMMARY:**

Multiple vulnerabilities have been discovered in Cisco Telepresence TC and TE software which is the software used by Cisco Telepresence systems. The affected appliances provide remote presence systems for businesses . It should be noted that these vulnerabilities are independent of one another. In other words, a Cisco Telepresence system that is affected by one of these vulnerabilities may not be affected by the others.

Please see the following link to Cisco's advisory and find the sub-menu for "Software Versions and Fixes" to find a detailed graph describing which versions of the Cisco Telepresence Software is affected by which vulnerability:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140430-tcte>

The following vulnerabilities have been identified:

- Multiple remote denial-of-service vulnerabilities exist as the software fails to properly handle SIP packets. Specifically, these issues affect the SIP code.
- A buffer-overflow vulnerability exists in the implementation of the DNS code. The issue occurs due to insufficient bounds check on variables. An attacker can exploit this issue by injecting specially crafted DNS response packets.
- A command-injection vulnerability exists due to an error in the implementation of internal system scripts. The issue occurs due to improper validation of parameters passed to the affected system scripts.

- A command-injection vulnerability exists due to an error in the implementation of several system scripts.
- A heap-based buffer-overflow vulnerability exists in the SIP code. An attacker can exploit this issue by sending specially crafted SIP packets.
- A local buffer-overflow vulnerability exists in the implementation of executable utilities that use the universal 'bootloader' (u-boot) compiler.
- A local authentication-bypass vulnerability because it allows the user to connect to the serial port and obtain privileged access.
- A remote denial-of-service vulnerability exists in the H.225 code. An attacker can exploit this issue by sending specially crafted H.225 packets.

## **RECOMMENDATIONS:**

The following actions should be taken:

- Apply software updates provided by Cisco, and workarounds that mitigate these vulnerabilities are also available from Cisco at the following link: <http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140430-tcte>

## **REFERENCES:**

### **Cisco:**

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140430-tcte>

### **Security Focus:**

<http://www.securityfocus.com/bid/67170>

### **CVE:**

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-2162>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-2163>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-2164>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-2165>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-2166>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-2167>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-2168>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-2169>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-2170>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-2171>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-2172>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-2173>