

*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:**

07/31/2013

**SUBJECT:**

Authenticated Command Injection Vulnerability in Multiple Cisco Content Network and Video Delivery Products

**OVERVIEW:**

Multiple Cisco content network and video delivery products contain a vulnerability when they are configured to run in central management mode. This vulnerability could allow an authenticated but unprivileged, remote attacker to execute arbitrary code on the affected system and on the devices managed by the affected system.

**SYSTEMS AFFECTED:**

- Cisco Wide Area Application Services (WAAS)
- Cisco Application and Content Networking System (ACNS)
- Cisco Enterprise Content Delivery System (ECDS)
- Cisco Internet Streamer Content Delivery System (CDS-IS)
- Cisco VideoScape Delivery System for Internet Streamer (VDS-IS)
- Cisco Videoscape Distribution Suite Service Broker (VDS-SB)
- Cisco Videoscape Distribution Suite Optimization Engine (VDS-OE)
- Cisco VideoScape Delivery System Origin Server (VDS-OS)

(see advisory for specific versions affected)

**RISK:**

**Government:**

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

**Businesses:**

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

**Home users: Low**

**DESCRIPTION:**

A vulnerability in the web framework could allow an authenticated, remote attacker to execute arbitrary commands on the underlying operating system of the affected system as well as on underlying operating system of the devices associated and managed by the affected system.

The vulnerability is due to a failure to properly sanitize user input that is subsequently used to perform an action using the underlying command-line interface of the device. An authenticated but unprivileged attacker could exploit this vulnerability by logging in to the GUI of the affected system and appending arbitrary code to some of values passed to the system.

**RECOMMENDATIONS:**

The following actions should be taken:

- Update the devices on vulnerable systems using the instructions provided by Cisco  
<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130731-cm>

**REFERENCES:****Cisco:**

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130731-cm>