

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:

10/09/2013

SUBJECT:

Multiple Vulnerabilities in Cisco FWSM Software Could Allow Remote Access or Denial of Service

OVERVIEW:

Multiple vulnerabilities have been discovered in Cisco Firewall Services Module (FWSM) Software for Cisco Catalyst 6500 Series Switches and Cisco 7600 Series Routers. Cisco FWSM software provides firewall services. Successful exploitation of the Cisco FWSM Command Authorization Vulnerability may result in a complete compromise of the confidentiality, integrity and availability of the affected system. Successful exploitation of the SQL*Net Inspection Engine Denial of Service Vulnerability may result in a reload of an affected device, leading to a denial of service (DoS) condition.

SYSTEMS AFFECTED:

Cisco FWSM Software for Cisco Catalyst 6500 Series Switches and Cisco 7600 Series Routers

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

DESCRIPTION:

Multiple vulnerabilities have been discovered in Cisco Firewall Services Module (FWSM) Software for Cisco Catalyst 6500 Series Switches and Cisco 7600 Series Routers. The Cisco

FWSM is a high-speed, integrated firewall module for Cisco Catalyst 6500 Series Switches and Cisco 7600 Series Routers. The FWSM offers firewall services with stateful packet filtering and deep packet inspection. Successful exploitation of the Cisco FWSM Command Authorization Vulnerability may result in a complete compromise of the confidentiality, integrity and availability of the affected system. Successful exploitation of the SQL*Net Inspection Engine Denial of Service Vulnerability may result in a reload of an affected device, leading to a denial of service (DoS) condition.

These vulnerabilities are independent of one other; a release that is affected by one of the vulnerabilities may not be affected by the other.

Cisco FWSM Command Authorization Vulnerability

A vulnerability in the authorization code of the Cisco Firewall Services Module (FWSM) could allow an authenticated but unprivileged, local attacker to delete, modify, or view the configuration of any other context of the affected system.

SQL*Net Inspection Engine Denial of Service Vulnerability

The SQL*Net protocol consists of different packet types that the SQL*Net inspection engine of the Cisco FWSM controls to make the data stream appear consistent with the Oracle applications on either side of the firewall.

RECOMMENDATIONS:

The following actions should be taken:

Upgrade vulnerable Cisco products immediately after appropriate testing.

REFERENCES:

CISCO:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20131009-fwsm>

<http://tools.cisco.com/security/center/viewAlert.x?alertId=31097>

<http://tools.cisco.com/security/center/viewAlert.x?alertId=31098>