

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:

10/11/2012

SUBJECT:

Multiple Vulnerabilities in Cisco Products Could Allow the Execution of Arbitrary Commands or Denial of Service

OVERVIEW:

Multiple vulnerabilities have been discovered in Cisco products including Cisco Adaptive Security Appliances (ASA) 5500 Series and Cisco Catalyst 6500 Series ASA Services Module. Cisco ASA products provide firewall, intrusion prevention, remote access, and other services. Successful exploitation of one of the vulnerabilities could lead to an attacker executing arbitrary commands on the system. The remaining vulnerabilities could result in denial of service conditions or a reload on the affected device.

SYSTEMS AFFECTED:

Cisco ASA 5500 Series Adaptive Security Appliances (ASA)
Cisco Catalyst 6500 Series ASA Services Module (ASASM)

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 ASA 5500 series appliances and Cisco Catalyst 6500 Series ASA Service Modules (ASASM). Successful exploitation of one of the vulnerabilities could lead to an attacker executing arbitrary commands on the system. The remaining vulnerabilities could result in denial of service conditions or a reload on the affected device.

The details of each vulnerable Cisco product are provided below.

DCERPC Inspection Buffer Overflow Vulnerability

A vulnerability exists in the DCERPC inspection engine that would allow an unauthenticated, remote attacker to cause a reload of the affected system or to overflow the stack, and possibly execute arbitrary commands. The vulnerability is due to insufficient validation of DCERPC packets within a valid DCERPC session. An attacker could exploit this vulnerability by sending a crafted DCERPC packet that needs to be inspected by the affected system. This issue is being tracked by Cisco bug ID CSCtr21359 (CVE-2012-4661).

DHCP Memory Allocation Denial of Service Vulnerability

A DHCP memory allocation denial of service vulnerability exists in the implementation of the Dynamic Host Configuration Protocol (DHCP) Server. This vulnerability could allow an unauthenticated, remote

attacker to trigger a reload of the affected device. This vulnerability is due to a failure in allocating memory for an internal DHCP data structure upon receiving specially crafted DHCP packets. An attacker could exploit this vulnerability by sending a sequence of specially crafted DHCP packets to the affected system. This issue is being tracked by Cisco bug ID CSCtw84068 (CVE-2012-4643).

SSL VPN Authentication Denial of Service Vulnerability

An SSL VPN authentication denial of service vulnerability exists in the implementation of the authentication, authorization and accounting (AAA) code for remote the SSL VPN (Clientless and AnyConnect) feature. This vulnerability could allow an unauthenticated, remote attacker to trigger a reload of the affected system. This vulnerability is due to insufficient validation of a crafted authentication response when an AAA challenge-response is required to complete the authentication process. An attacker could exploit this vulnerability by trying to authenticate on an ASA configured for SSL VPN with a crafted authentication challenge response. This issue is being tracked by Cisco bug ID CSCtz04566 (CVE-2012-4659).

SIP Inspection Media Update Denial of Service Vulnerability

A vulnerability exists in the SIP inspection engine code of the Cisco ASA Software may allow an unauthenticated, remote attacker to trigger a reload of the affected device. This vulnerability is due to improper processing of SIP media update packets. An attacker could exploit this vulnerability by sending a specially crafted SIP packet through the affected system. This issue is being tracked by Cisco bug ID CSCtr63728 (CVE-2012-4660).

Two DCERPC Inspection Denial Of Service Vulnerabilities

Two vulnerabilities exist in the DCERPC inspection engine that would allow an unauthenticated, remote attacker to cause a reload of the affected system. The vulnerabilities are due to insufficient validation of DCERPC packets within a valid DCERPC session. An attacker could exploit this vulnerability by sending a crafted DCERPC packet that needs to be inspected by the affected system. These issues are being tracked by Cisco bug IDs CSCtr21376 and CSCtr21346 (CVE-2012-4662 and CVE-2012-4663).

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-20121010-asa>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-4643>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-4659>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-4660>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-4661>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-4662>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-4663>

SecurityFocus:

<http://www.securityfocus.com/bid/55861>

<http://www.securityfocus.com/bid/55862>

<http://www.securityfocus.com/bid/55863>

<http://www.securityfocus.com/bid/55864>

<http://www.securityfocus.com/bid/55865>