

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:

02/24/2011

SUBJECT:

Vulnerability Cisco NX-OS Software Could Allow Denial of Service Vulnerability (cisco-sa-20120215-nxos)

OVERVIEW:

Cisco NX-OS Software is affected by a denial of service (DoS) vulnerability that could cause Cisco Nexus 1000v, 5000, and 7000 Series Switches that are running affected versions of Cisco NX-OS Software to reload when the IP stack processes a malformed IP packet.

SYSTEMS AFFECTED:

- Cisco Nexus 1000v, 5000, and 7000 Series Switches

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

DESCRIPTION:

Certain versions of Cisco NX-OS Software for Cisco Nexus 1000v, 5000, and 7000 Series Switches are affected by a vulnerability that may cause a reload of an affected device when the operating system's IP stack processes a malformed IP packet and obtaining Layer 4 (UDP or TCP) information from the packet is required. The vulnerability is in the operating system's IP stack and any feature that makes use of services offered by the IP stack to parse IP packets is affected.

Successful exploitation of the vulnerability that is described in this advisory may result in a reload of an affected device. Repeated exploitation could result in a sustained DoS condition.

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate updates provided by Cisco to vulnerable systems immediately after appropriate testing.

REFERENCES:

Cisco:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120215-nxos>

CVE:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0352>