

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.

TLP: WHITE

Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.

<http://www.us-cert.gov/tlp/>

DATE(S) ISSUED:

01/14/2016

SUBJECT:

Multiple Vulnerabilities in Cisco Products Could Allow for Unauthenticated, Remote Access

OVERVIEW:

Multiple vulnerabilities have been discovered in Cisco products including Aironet 1800 Series Access Points, Wireless LAN Controller software, and Identity Services Engine software. Successful exploitation could potentially allow an attacker to take control of the affected system and perform unauthorized actions.

THREAT INTELLIGENCE:

There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:

- Cisco Aironet 1830e Series Access Point
- Cisco Aironet 1830i Series Access Point
- Cisco Aironet 1850e Series Access Point
- Cisco Aironet 1850i Series Access Point
- Cisco 2500 Series Wireless Controllers
- Cisco 5500 Series Wireless Controllers
- Cisco 8500 Series Wireless Controllers
- Cisco Flex 7500 Series Wireless Controllers
- Cisco Virtual Wireless Controllers
- Cisco Identity Services Engine and Identity Services Engine Express versions 1.1 or later, 1.2.0 prior to patch 17, 1.2.1 prior to patch 8, 1.3 prior to patch 5, or 1.4 prior to patch 4

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

TECHNICAL SUMMARY:

Cisco Products are prone to multiple vulnerabilities that could allow for unauthorized access. These vulnerabilities are as follows:

- An unauthorized access vulnerability in devices running Cisco Wireless LAN Controller (WLC) software versions 7.6.120.0 or later, 8.0 or later, or 8.1 or later that could allow an unauthenticated, remote attacker to modify the configuration of the device. (CVE-2015-6314)
- An unauthorized access vulnerability in the Admin portal of devices running Cisco Identity Services Engine (ISE) software that could allow an unauthenticated, remote attacker to gain unauthorized access to an affected device. (CVE-2015-6323)
- A vulnerability in Cisco Aironet 1800 Series Access Point devices that could allow an unauthenticated, remote attacker to log in to the device by using a default account that has a static password. (CVE-2015-6336)

RECOMMENDATIONS:

The following actions should be taken:

- Install the updates provided by Cisco immediately after appropriate testing.
- Verify no unauthorized system modifications have occurred on system before applying patch.
- Monitor intrusion detection systems for any signs of anomalous activity.
- Unless required, limit external network access to affected products.

REFERENCES:

Cisco

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160113-wlc>

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160113-ise>

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160113-air>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6314>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6323>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6336>

TLP: WHITE

Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.

<http://www.us-cert.gov/tlp/>