

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:**

01/13/2015

**01/25/2016 - UPDATED**

**SUBJECT:**

Vulnerability in Fortinet FortiOS Could Allow Unauthorized Remote Access

**OVERVIEW:**

A vulnerability has been discovered in Fortinet FortiOS that could allow unauthorized remote administrative access to the device if the device has "Administrative Access" enabled for SSH. FortiOS is the operating system used by FortiGate network security platforms. Successful exploitation could lead to remote administrative access of an impacted FortiOS device.

**THREAT INTELLIGENCE:**

Exploit script freely available on the Internet.

**SYSTEMS AFFECTED:**

- FortiOS versions 4.3.0 to 4.3.16
- FortiOS versions 5.0.0 to 5.0.7

**January 23 - UPDATED SYSTEMS AFFECTED:**

- **FortiAnalyzer: 5.0.5 to 5.0.11 and 5.2.0 to 5.2.4 (branch 4.3 is not affected)**
- **FortiSwitch: 3.3.0 to 3.3.2**
- **FortiCache: 3.0.0 to 3.0.7 (branch 3.1 is not affected)**
- **FortiOS 4.1.0 to 4.1.10**
- **FortiOS 4.2.0 to 4.2.15**

**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:**

A vulnerability has been discovered in Fortinet FortiOS that could allow unauthorized, remote administrative access to the device if the device has “Administrative Access” enabled for SSH. Successful exploitation could lead to remote administrative access of an impacted FortiOS device.

The vulnerability identified could lead to remote administrative access via SSH of a FortiOS device, resulting in the complete compromise of the impacted system. A hard-coded password exists in the firewall software that would allow a remote attacker to login with full administrative access to the device by using the “Fortimanager\_Access” username and a hashed version of the string “FGTAbc11\*xy+Qqz27” as the password.

#### **RECOMMENDATIONS:**

The following actions should be taken:

- Disable administrator access over SSH on all the network interfaces of the device and use the Web GUI or console applet for the GUI instead.
- In cases where SSH access is necessary in FortiOS 5.x versions, restrict SSH access to minimal set of pre-authorized IP addresses.
- Apply appropriate patches provided by Fortinet to vulnerable systems immediately after appropriate testing.

#### **REFERENCES:**

##### **Fortiguard Center:**

<https://www.fortiguard.com/advisory/fortios-ssh-undocumented-interactive-login-vulnerability>

##### **Security Affairs:**

<http://securityaffairs.co/wordpress/43551/hacking/fortinet-fortios-ssh-backdoor.html>

##### **Security Week:**

<http://www.securityweek.com/fortinet-denies-existence-malicious-backdoor-fortios>

##### **January 23 - UPDATED REFERENCES:**

##### **Fortinet:**

<http://blog.fortinet.com/post/ssh-issue-update>

#### **TLP: WHITE**

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

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