Subject: **SSH Login Vulnerability in Fortinet Products (Advisory No 05 Feb 2016)**

1. **Introduction.** An undocumented account used for communication with authorized FortiManager devices exists on some versions of FortiOS, FortiAnalyzer, FortiSwitch and FortiCache. On vulnerable versions if "Administrative Access" is enabled for SSH, this account can be used to log in via SSH in Interactive-Keyboard mode, using a backdoor (password) shared across all devices. It gives access to a CLI console with administrative rights.

2. **Impact.** Any user within LAN can access the devices and view / change the configuration of devices.

3. **Affected Products.** Devices affected by the vulnerability are listed below:-

a. FortiAnalyzer 5.0.5 to 5.0.11 and 5.2.0 to 5.2.4 (branch 4.3 is not affected).

b. FortiSwitch 3.3.0 to 3.3.2.

c. FortiCache 3.0.0 to.3.0.7 (branch 3.1 is not affected).

d. FortiOS 4.1.0 to 4.1.10.

e. FortiOS 4.2.0 to 4.2.15.

f. FortiOS 4.3.0 to 4.3.16.

g. FortiOS 5.0.0 to 5.0.7.

4. **Recommendation**

a. **Workarounds.** The following workarounds should be performed on the devices to temporarily fix the problem:-

(1) **FortiAnalyzer.** Restrict access to the administration interfaces (including SSH access) to a minimal set of authorized IP addresses, via the trusthost commands.

(2) **FortiSwitch.** Disable admin access via SSH on all interfaces, and use the Web GUI instead, or the console applet of the GUI for CLI access.

(3) **FortiCache**

(a) Disable admin access via SSH on all interfaces, and use the Web GUI instead, or the console applet of the GUI for CLI access.

Page Contd...2

(b) If management by a FortiManager device is not needed, the CLI commands may be disabled

(4) **FortiOS**

(a) Disable admin access via SSH on all interfaces, and use the Web GUI instead, or the console applet of the qui for CLI access.

(b) On 5.0 and 4.3, if SSH access is mandatory, restrict access to SSH to a minimal set of authorized IP addresses, via the Local In policies.

(c) On 4.2 and 4.1, if SSH access is mandatory, restrict access to the administration interfaces (including SSH access) to a minimal set of authorized IP addresses, via the trusthost commands.

(d) If management by a FortiManager device is not needed, the CLI commands (Attached as Annex A) disable access with the undocumented account

b. **Mitigation Measures.** In order to mitigate effect of vulnerability, following measures should be adopted:-

(1) **Forti Analzer.** Upgrade to 5.0.12 or 5.2.5.

(2) **Forti Switch.** Upgrade to 3.3.3.

(3) **Forti Cache.** Upgrade to 3.0.8 or to branch 3.1.

(4) **Forti OS.** Upgrade to any of the currently available versions i.e. 4.1.11, 4.2.16, 4.3.17 or later in branch 4.3, 5.0.8 or later in branch 5.0, 5.2.0 or later in branch 5.2, 5.4.0.