Number:	CSB-160115-1
Released:	15th Jan 2016
Modified:	20th Jan 2016
Subject:	SSH Undocumented Interactive Login Vulnerability
Product:	FortiGate, FortiAnalyzer, FortiCache, FortiSwitch

Description:

A device management authentication vulnerability exists in affected products which could allow unauthorized users to obtain remote console access to affected devices when "Administrative Access" is enabled for SSH.

The predefined account used is Fortimanager_Access for **all affected products except FortiSwitch for which the account is FortiLink (a read-only account).** Although successful login attempts using these accounts are not recorded in the event logs, configuration changes using these accounts are.

Possibly Affected Products:

All FortiGate models running the following FortiOS versions
FortiOS 4.1.0 to 4.1.10
FortiOS 4.2.0 to 4.2.15
FortiOS 4.3.0 to 4.3.16
FortiOS 5.0.0 to 5.0.7

FortiAnalyzer models running FortiAnalyzer 5.0 & 5.2
FortiCache models running FortiCache 3.0.0 to 3.0.7
FortiSwitch models running FortiSwitch 3.3.0 to 3.3.2

Remedy:

FortiOS branch 4.1: Upgrade to FortiOS 4.1.11 or later

FortiOS branch 4.2: Upgrade to FortiOS 4.2.16 or later

FortiOS branch 4.3: Upgrade to FortiOS 4.3.17 or later

FortiOS branch 5.0: Upgrade to FortiOS 5.0.8 or later

FortiAnalyzer 5.0: Upgrade to FortiAnalyzer 5.0.12

FortiAnalyzer 5.2: Upgrade to FortiAnalyzer 5.2.5

FortiCache 3.0: Upgrade to FortiCache 3.0.8

FortiSwitch 3.3: Upgrade to FortiSwitch 3.3.3

Workarounds:

Any of the following workarounds may be used.

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

config system interface
edit <interface name>
set allow < management protocols ….. do not include ssh >

2. Restrict using Trusted Host

If SSH access is mandatory, restrict access for all configurable administrative accounts to specific trusted host IP addresses.

config sys admin
edit <admin account>
set trusthost1 <IP address or subnet range>

3. Local-In Policy (FortiOS only)

If SSH access is mandatory, in FortiOS you can restrict access to SSH to a minimal set of authorized source IP addresses, via the Local In Policy feature.

SSH Access permitted for allowed host addresses
config firewall local-in-policy
edit 1
set intf <interface>
set srcaddr <address objects for allowed host addresses>
set dstaddr "all"
set action accept
set service "SSH"
set schedule "always"
next

SSH Access denied for all other host IP addresses

edit 2
set intf <interface>
set srcaddr "all"
set dstaddr "all"
set service "SSH"
set schedule "always"
end

4. Disable FortiManager Management (FortiOS only)

If management by a FortiManager device is not needed, the following CLI commands disable access with the undocumented account:

config system central-management
set type fortiguard
end

Customers who do not have valid support coverage for their products will be allowed to download firmware required to remedy the vulnerability. To download firmware in this way, please contact Customer Service.

For future updates, please consult the following FortiGuard advisory:
http://www.fortiguard.com/advisory/fortios-ssh-undocumented-interactive-login-vulnerability

Technical Support Contact Information: http://www.fortinet.com/support/contact_support.html
Fortinet technical support home page: https://support.fortinet.com