## Advisory Detail

**Date: 22/08/2016**

**Advisory Name: Shadow Brokers and Cisco Systems.**

**Overview :**

A mysterious group named "The Shadow Brokers" compromised a group named "Equation Group", a hacking group believed to be a NSA offshoot for a long time. They have publicly released exploits developed by them. Some of the exploits have been made available free as a Proof and the others believed to be of high value are available on an auction. One of the multiple vendors that has been impacted by this disclosure is Cisco, which is globally deployed on a large scale. [1]

The following advisory is aimed to study how Cisco was affected by "The Shadow Brokers". Two main products were targeted, Cisco ASA and legacy Cisco PIX firewalls.

**High Risk :**

The disclosure by Shadow Brokers includes exploitation source code which is now publicly available over the Internet. Two main products that are impacted by this disclosure are the Cisco PIX and Cisco ASA firewalls which form the first line of defense for many organizations.

The code could allow anyone with basic knowledge (script kiddies) to carry out an exploitation against any Cisco appliance raising the Risk level to **High**.

Additionally, Cisco devices have been deployed widely across critical sectors / systems in the State of Qatar, which increases the risk level further.

**Vulnerabilities :**

The code / exploits published by the "Shadow Brokers" to exploit Cisco appliances uses the following vulnerabilities:

1. Cisco ASA SNMP Remote Code Execution Vulnerability (Severity level: **High**). A vulnerability in the Simple Network Management Protocol (SNMP) code of Cisco Adaptive Security Appliance (ASA) Software could

[1] http://blog.trendmicro.com/tippingpoint-threat-intelligence-zero-day-coverage-week-august-15-2016/

allow an authenticated, remote attacker to reload the affected system or to execute code remotely. Vulnerability was published first time on 17th August 2016 at 18:45GMT with **CVE-2016-6366** which means after the Shadow Brokers was released. A full Cisco Security Advisory including workaround in the following link and still working on fixes :-

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160817-asa-snmp

2. Cisco ASA CLI Remote Code Execution Vulnerability (Severity level: **Medium**) A vulnerability in the command-line interface (CLI) parser of Cisco Adaptive Security Appliance (ASA) Software could allow an authenticated local attacker to create a denial of service (DoS) incident or potentially execute arbitrary code. An attacker could exploit this vulnerability by invoking certain invalid commands to the affected device. Vulnerability was published by first time in 17th August 2016 at 18:45GMT with **CVE-2016-6366**. A full Cisco Security Advisory including workaround and fixes in the following link :-

   http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160817-asa-cli

3. Other Cisco vulnerabilities that have been discovered on the same date and not related to "Shadow Brokers" are:
   a. Cisco Firepower Management Center Privilege Escalation Vulnerability.
   b. Cisco Firepower Management Center Remote Command Execution Vulnerability.
   c. Cisco Application Policy Infrastructure Controller Enterprise Module Remote Code Execution Vulnerability.
   d. Cisco Aironet 1800, 2800, and 3800 Series Access Point Platforms AMPDU Denial of Service Vulnerability.
   e. Cisco Aironet 1800, 2800, and 3800 Series Access Point Platforms CLI Privilege Escalation Vulnerability.
   f. Cisco Aironet 1800, 2800, and 3800 Series Access Point Platforms 802.11 Protocol Denial of Service Vulnerability.
   g. Cisco Firepower Management Center Cross-Site Scripting Vulnerability.
   h. Cisco IP Phone 8800 Series Denial of Service Vulnerability
   i. Cisco Identity Services Engine Admin Dashboard Page Cross-Site Scripting Vulnerability.

j. Cisco Smart Call Home Transport Gateway Cross-Site Scripting Vulnerability.
k. Cisco Unified Communications Manager Information Disclosure Vulnerability.
l. Cisco WebEx Meetings Server Information Disclosure Vulnerability.

All details required for such vulnerabilities can be found on the following link :-

https://www.us-cert.gov/ncas/current-activity/2016/08/20/Cisco-Releases-Security-Updates

**General Recommendation :**

Cisco published an online page "**Cisco ASA Integrity Assurance**" that provides guidance on how to perform the following integrity assurance :-

- Cisco ASA image file verification.
- Cisco ASA runtime memory integrity verification with core dumps and creating known-good text regions.
- Checking external accounting logs.
- Checking external syslog logs.
- Checking booting information.
- Checking the ROMMON information.
- Checking failover events.
- Checking the SSL VPN portal code.
- Checking integrity of SSL VPN plugins.
- Checking the configuration checksum.
- Verify the integrity of other software loaded on the Cisco ASA.

All details required for **Integrity Assurance** can be found on the following link :-
http://www.cisco.com/c/en/us/about/security-center/intelligence/asa-integrity-assurance.html

**Further Inquiry :**

Q-CERT Team is be available for any inquiry or emergency response on 24x7 basis through the following contacts:

- Q-CERT Hotline: **+974 - 44933408 / +974 – 44995399**.
- Q-CERT E-Mail: indcidents@qcert.org