GOVERNMENT OF PAKISTAN
CABINET SECRETRIAT, CABINET DIVISION
NATIONAL TELECOM & INFORMATION TECHNOLOGY SECURITY BOARD
(NTISB-II)

359

No. 1-5/2003 (NTISB-II) Islamabad 30 April, 2018

Subject: **Advisory Prevention Against Cyber Espionage (Advisory No 120)**

1. **Introduction.** A new vulnerability has been disclosed in iOS Camera App that could be exploited to redirect users to a malicious website without their knowledge. The vulnerability affects Apple's latest iOS 11 mobile operating system for iPhone/ iPad/ iPod touch devices and resides in the built-in OR code reader.

M (A)
M (I.T)
A.S (Rev. Div)

2. **Technical Analysis**

a. With iOS 11, Apple introduced a new feature that gives users ability to automatically read QR codes using their iPhone's native camera app without requiring any third-party QR code reader app.

b. You need to open the Camera app on your iPhone or iPad and point the device at a OR code. If the code contains any URL, it will give you a notification with the link address, asking you to tap to visit it in Safari browser.

c. The URL parser of built-in QR code reader for iOS camera app fails to detect the hostname in the URL, which allows attackers to manipulate the displayed URL in the notification, tricking users to visit malicious websites instead.

Cep 9/5
a(IT)

3. **Affected Products.** This vulnerability affects all versions of iPhone, iPad and iPod till update.

4. **Recommendations**

a. Keep iOS firmware up to date.

b. Don't jailbreak your iPhone and only install applications with good reputation from Apple app store

c. Don't download attachments from emails unless you are sure about the source.

5. Forwarded for perusal and dissemination of information to all concerned, please.

For circulation & posting on web.
9-5-18

Major
(Iftikhar Ali)
Assistant Secretary (NTISB-II)
Ph# 051-9204560

All Secretaries of Ministries / Divisions of Federal Government and PSO to Chief Secretaries of Provincial Governments

10-5.

webmaster

Sec-IT

put up Asstt Dir 10/5

CABINET SECRETRIAT, CABINET DIVISION
NATIONAL TELECOM & INFORMATION TECHNOLOGY SECURITY BOARD
(NTISB-II)

352

No. 1-5/2003 (NTISB-II) Islamabad 30 April, 2018

M(A)
M(I.T)
A.S (Rev.Div)

Subject: **Advisory - Prevention Against Cyber Espionage (Advisory No 121)**

1. **Introduction.** Recently reports have indicated that attackers from Iran are using latest malware techniques **to distribute macro-based documents to individuals in Asia and Middle East**. These attackers are **focusing Pakistan Defense Institutions** and **utilize crafted spear-phishing emails** with **attached malicious word documents.** Downloading and opening the file from email **executes the malware in background** and **opens a fake document in foreground**, that results in **hacking of the system.**

2. **Summary of Malicious Email**

a. **Subjects of Reported Emails**

(1) National Assembly of Pakistan
(2) Turkish Armed Forces
(3) State Bank of Pakistan

For circulation + posting on web
9-5-18
Sec IT
105
webmaster

b. **Name of Attachments**

(1) Important Notice: National Assembly.doc
(2) Turkish vs Pakistan Armed Forces.doc
(3) na.gov.pk.doc
(4) Invest in Turkey.doc

cl(IT)

c. **Malware Type.** Macro based Malware with Remote Access Trojan capability.

d. **Infection Vector.** Spear Phishing Emails.

e. **Targeted Countries.** Turkey, Pakistan, Tajikistan.

3. **Indicators of Compromise.** The malware creates following files in hardcoded paths into the infected system:-

a. C:\ProgramData\Defender.sct (A malicious JavaScript file).

b. C:\ProgramData\DefenderService.inf (To execute JavaScript file).

c. C:\ProgramData **MindowsDefender.ini** (Malicious PowerShell script).

d. **\REGISTRY\USEMSID1Software1Microsoft\Windows\CurrentVersion \Run\"WindowsDefenderUpdater"** =cmstp.exe /s c:\programdat \ **DefenderService.inf** (Registry Key for Persistence).

C 349

GOVERNMENT OF PAKISTAN
CABINET SECRETRIAT, CABINET DIVISION
NATIONAL TELECOM & INFORMATION TECHNOLOGY SECURITY BOARD
(NTISB-II)

No. 1-5/2003 (NTISB-II) **Islamabad 30 April, 2018**

Subject: **Advisory Prevention Against Cyber Espionage (Advisory No 122)**

1. **Introduction.** A hacking group named **`JHT'** hijacked a significant number of Ciscodevices belonging to organizations in **Russia/ Iran** and left a message that reads "Do not mess with our elections" with an American flag. This campaign impacted approximately 3,500 network switches in Iran though a majority of them were already restored.

2. **Technical Analysis**

M (A)
M (I.T)
A.S (Rev. Div)

a. The attack involves recently disclosed remote code execution vulnerability **(CVE-2018-0171)** in Cisco Smart Install Client that could allow attackers to take full control of the network equipment.

b. The Cisco Smart Install protocol can be abused to modify the TFTP server setting, exfiltrate configuration files via TFTP, modify the configuration file, replace the 105 image and setup accounts allowing for the execution of IOS commands.

c. According to the scanning engine Shodan, more than 165,000 systems are still exposed on the Internet.

3. **Affected Products.** Catalyst 4500 Supervisor Engines, Cisco Catalyst 3850 Series Switches and Cisco Catalyst 2960 Series Switches devices, as well as all devices that fall into the Smart Install Client type are potentially vulnerable.

4. **Recommendations.**

a. Administrators who have install the Cisco Smart Install feature, should disable it entirely with the configuration command — "no vstack".

b. Network administrators are highly recommended to install patches to address this vulnerability (CVE-2018-0171).

915
CIT

5. Forwarded for perusal and dissemination of information to all concerned,please..

For circulation & posting on web 9.5.18
Sec-IT

Major
(Iftikhar Ali)
Assistant Secretary (NTISB-II)
Ph# 051-9204560

All Secretaries of Ministries / Divisions of Federal Government and PSO to Chief Secretaries of Provincial Governments

10.5.18
webmaster

GOVERNMENT OF PAKISTAN
CABINET SECRETRIAT, CABINET DIVISION
NATIONAL TELECOM & INFORMATION TECHNOLOGY SECURITY BOARD
(NTISB-II)

No. 1-5/2003 (NTISB-II) **Islamabad** 30 **April, 2018**

Subject: **Advisory Prevention Against Cyber Espionage (Advisory No 123)**

1. **Introduction.** Recently, a group of serious vulnerabilities have been disclosed by Microsoft that an allow the hackers to remotely take control of the system by just clicking on the malicious link or by just opening website. This vulnerability affects all versions of Windows operating systems to date.

2. **Technical Details.**

M(A)
M(I.T)
A.S(Rev. Div)

a. An attacker can exploit these issues by tricking the user to open a malicious file or a specially crafted website with the malicious font, which if open in a web browser would hand over control of the affected system to the attacker or it can stop responding to the user.

b. Microsoft has patched these critical vulnerabilities in Windows Graphics Component that reside in the operating system due to improper handling of embedded fonts by the Windows font library.

c. These five vulnerabilities found in Windows Microsoft Graphics are listed below:-

(1) CVE-2018-1010
(2) CVE-2018-1012
(3) CVE-2018-1013
(4) CVE-2018-1015
(5) CVE-2018-1016

10.5.18
webmaster

56928

9/5
C(IT)

3. **Affected Products.** These vulnerabilities affect the following versions of Microsoft Products:-

a. Windows 7, 8.1, RT 8.1 and 10.

b. Windows Server 2008, 2012 and 2016.

4. **Recommendations.**

a. Install and update well reputed antivirus such as Kaspersky, Bitdefender, Nod 32and Avast etc.

b. Update all softwares including Windows OS, Microsoft Office and all other softwares. For updating windows to Setting → Update & Security → Windows Update → Check for updates.

c. Don't download attachments from emails unless you are sure about the source.

6. Forwarded for perusal and dissemination of information to all concerned, please.

For circulation & posting on the website
9.5.18
Secretary IT

Major
(Iftikhar Ali)
Assistant Secretary (NTISB-II)
Ph# 051-9204560

All Secretaries of Ministries / Divisions of Federal Government and PSO to Chief Secretaries of Provincial Governments