Please put up on file - 28/12/2017

Dir(OT)

APS

GOVERNMENT OF PAKISTAN
PAKISTAN METEOROLOGICAL DEPARTMENT
(HEADQUARTER OFFICE)
P. O. BOX NO.1214, SECTOR H-8/2,
ISLAMABAD

No. GA-21(46)/2013-1939 Islamabad, the 26 Dec. 2017

Pl. do the needful as required

CIRCULAR

Subjects: **ADVISORY – PREVENTION AGAISNT CICROSOFT SECURITY FLAWS (ADVISORY NO. 94).**

28/12/17

ADVISORY – PREVENTION AGAINST FAKE WHATSAPP ON GOOLE PAY STORE (ADVISORY NO. 97 DATED 13- NOV. 2017).

Programmer (IT)

ADVISORY – PREVENTION AGAINST CYBER EXPIONAGE (ADVISORY NO. 98).

Kindly find enclosed herewith a copies of National Telecom & Information Technology Security Board, letter No. 1(5)/2003(NTISB) dated 15th & 30th Nov. 20127 on the above subjects for information and further necessary action.

Encl: (As above)

Plz upload on website 29/12/17
S.E(Waqid)

(ALLAUDDIN)
SUPERINTENDENT

Distribution:-

1. Chief Met., Drought / R&D, Met. HQs. Office, Islamabad.
2. Chief. Met, FFD, Lahore / Karachi.
3. Director, RMC, Karachi / Lahore / Peshawar / Quetta / GB.
4. Syed Zeeshan Haider (Programmer) Please upload on PMD's Website.

Through PMD website

Chief Met. Office Dy. No. 0444 Date 28/12/2017

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

No. 1-5/2003 (NTISB-II) Islamabad 30 November, 2017

Subject: Advisory — Prevention Against Cyber Espionage (Advisory No. 98)

1. **Introduction.** A critical vulnerability of TOR browser has been identified by Italian security researcher Filippo Cavallarin. This vulnerability can leak real IP addresses of users to potential attackers, upon visiting certain types of web page.

2. **Affected Software.**
   a. The vulnerability affects Tor browser for mac OS and Linux. However it doesn't affect Windows users apparently.
   b. This vulnerability would affect the privacy and security of Tor users.

3. **Mode of operation.** Mode of operation is as under:-
   a. The vulnerability resides in Firefox that also affects Tor Browser, as the privacy-aware service that allows users to surf the web anonymously uses FireFox at its core.
   b. **TorMoil** bug, the vulnerability affects Tor browser. TorMoil is triggered when users click on links that begin with file:// addresses, instead of the more common https:// and http:// addresses.
   c. Once an affected user [running macOS or Linux system] navigates to a specially crafted web page, the operating system may directly connect to the remote host, bypassing Tor Browser

4. **Recommendations.** Following is suggested in this regard:-
   a. The Tor Project has currently issued a temporary workaround to prevent the real IP leakage.
   b. MacOS and Linux users may found the updated versions of the Tor anonymity browser that will not behave properly while navigating to file:// addresses, until a permanent patch becomes available.
   c. Regularly update the system with latest anti-virus.
   d. Update TOR to version 7.0.8.
   e. **Install and UPDATE well reputed antiviruses** such as Kaspersky, Bitdefender, Nod 32, Avast etc.
   f. Update all softwares including Windows OS, Internet browser (Mozilla,firfox) and microsoft office.
   g. Install and regularly update software firewall such as Comodo Firewall or Zonealarm.

Aviation Division
Section Officer (Admin)
Diary No. 1855 Date 8-12-17

Aviation Division
Deputy Secretary (Admin)
Diary No. 2532 Date 07-12-17

Aviation Division
Joint Secretary-III
Diary No. 2878 Date 7-12-17

Dy. No. 5582 SECY
DATED: 6.12.17

JS-III	JS-II	JS-I

JS/III

SECRET

8/12

DS (Admin) (AVL) S.O(A)

h. Don't click on any suspicious website popup during the Internet surfing. Don't download attachments from emails unless you are sure about the source.

5. **Reporting of Suspicious Files/Emails.** Any malicious activity may be reported to this organization on the following email address for analysis and suggesting mitigation measures:-

a. eagle1978@mail.com

b. falcon098@writeme.com

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

Major
(Iftikhar Ali)
Assistant Secretary (NTISB)

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

NATIONAL TELECOM & INFORMATION TECHNOLOGY SECURITY BOARD
(NTISB-II)

No. 1-5/2003 (NTISB-II) Islamabad 30 November, 2017

Subject: **Advisory -Prevention against Fake WhatsApp on Google Play Store (Advisory No. 97 Dated 13 Nov 2017)**

1. **Introduction.** Google Play Store is surrounded by hundreds of fake and malicious apps that trick users into downloading and installing them and potentially infect their smart phones to carry out malicious things without their knowledge. Recently, a fake version of the most popular WhatsApp messaging app for Android has been spotted by some users. The app named **Update WhatsApp Messenger** was uploaded on the official Google Play Store by an app developer who pretended to be the actual WhatsApp service with the developer title "WhatsApp Inc."—the same title the actual WhatsApp messenger uses on Google Play.

2. **Technique Used.** The app developer was able to use the same title as the legitimate maker of the WhatsApp by adding a Unicode character space after the actual WhatsApp Inc. name, which in computer code reads **WhatsApp+Inc%C2%A0.** This hidden character space at the end of the WhatsApp Inc. was invisible to an average Android user browsing Google Play Store, allowing this dodgy version of the app to masquerade as a product of WhatsApp Inc.

3. **Mode of Operation.** The app once downloaded will perform following actions:-

   a. Serve Android users with advisements to download other apps.

   b. The app will try to hide by not having a title and having a blank icon.

4. **Recommendations.** In order to prevent user's data from being vulnerable to theft, the following is suggested.

   a. Vigilantly download apps not only from the third-party app store but also from official Play Store in order to protect yourselves.

   b. Backup your files regularly.

   c. Scan system regularly with antivirus such as Kaspersky, Avira , Avast, ESET etc.

5. **Reporting of Suspicious Files/ Emails.** Any malicious email/file may be reported to this organization on the following email addresses for analysis and suggesting mitigation measures:-

   a. eagle1978gmail.com

   b. falcon098@writeme.com

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

Major
(Iftikhar Ali)
Assistant Secretary (NTISB)

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

SECRET

CABINET SECRETARIAT

NATIONAL TELECOM & INFORMATION TECHNOLOGY SECURITY BOARD
(NTISB-II)

No. 1-5/2003 (NTISB-II) Islamabad 15 November, 2017

Subject: **Advisory — Prevention Against Microsoft Security Flaws (Advisory No 94)**

1. **Introduction.** Various flaws namely CVE-2017-11826, CVE-2017-11779, CVE- 2017-8703 and CVE-2017-11826 have been discovered by security researchers. These flaws reside in various products of Microsoft, which can be exploited by sending a malicious code to an affected product.

2. **Maior Products Affected**

   a. All supported versions of MS Office.

   b. Windows DNS client.

   c. Windows Subsystem for Linux.

   d. Microsoft SharePoint Server.

3. **Impact.** The following flaws once exploited could allow an attacker to perform following activities:-

   a. **CVE-2017-11826.** Attacker could run arbitrary code in the context of the current user i.e. with the same rights as the logged in-user. So, **users with least privilege on their systems are less impacted than those having higher admin rights.**

   b. **CVE-2017-11779. Attacker can execute arbitrary code** on Windows clients or Windows Server installations in the context of the software application that made the DNS request.

   c. **CVE-2017-8703.** Attacker can execute a malicious application to affect an object in the memory, which eventually allows that the application **to crash the target system and made it unresponsive.**

   d. **CVE-2017-11826.** Attacker can **perform cross-site scripting (CSS) attacks** on affected systems and execute malicious script in the same

4. **Recommendations.** In order to prevent user's data from being vulnerable to theft, following is suggested:-

   a. Install **October security patches.** Go to Settings > Update & security > Windows Update > Check for updates and install them.

   b. **Backup your files regularly.**

   c. Download email attachments. only from trusted sources. **Even if a known contact sends a file,** open it after confirmation.

   d. Scan system regularly with **antivirus such as Kaspersky, Avira ,Avast, ESET** etc..

SECRET

Aviation Division
Section Officer (Admin)

Dy. No. 5191 SECY
DATED: 16-11-17
JS-III | Sr. JS-II | Sr. JS-I

e. Install well **reputed firewall with built-in HIPs** (Host Intrusion Prevention System).

5. **Reporting of Suspicious Files/Emails.** Any malicious activity may be reported to this organization on the following email address for analysis and suggesting mitigation measures:-

a. eagle1978@mail.com

b. falcon098@writeme.com

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

Major
(Iftikhar Ali)
Assistant Secretary (NTISB)

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