

F. No. 3(5)/2023-NTISB-EW
Government of Pakistan
Ministry of Science & Technology

Islamabad, the 28th September, 2023

Rector, COMSATS Islamabad	Chairman, PSF, Islamabad	Chairman, PCSIR, Islamabad	Chairman, PCST, Islamabad
Rector, NUST, Islamabad	Director General, NIO, Karachi	Director General, PSQCA, Karachi.	Chairman, PEC, Islamabad
Rector, NUTECH, Islamabad	Chairman, CWHR, Karachi	Director General, PNAC, Islamabad	Managing Director, STEDEC, Lahore.
Director General, PCRET, Islamabad	Director General, NIE, Islamabad	Managing Director, NEECA, Islamabad	Director General, PHA, Islamabad

Subject:

Cyber Security Advisory – Latest Android Patches/Updates/Fixing Zero Day Vulnerabilities (Advisory No. 55)

Cyber Security Advisory – Apple iPhones Targeted with Blast Pass Exploit to Deploy Pegasus Spyware (Advisory No. 56)

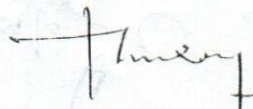
Cyber Security Advisory –Adobe Acrobat Reader Critical Vulnerabilities Patch Available (Advisory No. 58)

Cyber Security Advisory – Google Chrome Version Updated (Advisory No. 59)

Dear Sir / Madam,



Please find enclose herewith the subject advisories received from National Telecom and Information Technology Security Board (NTISB) Cabinet Division, for information and strict compliance.

Encl: **As above.**


(Kamran Nawaz Khan)
Deputy Electronics Adviser-I
051-9216304

Copy for information to:

- I. Network Administrator, MoST
- II. APS to JEA, MoST

Central Registry NUTECH	
Rector	
✓ Pro-Rector	
Dy Dir (Coord)	
GSO-1 (Coord)	
Head Clk	
Dte/Office	107
Diary No	3471
Date	

circulate
to all by
Registrar



Registrar Office NUTECH	
Rector	-
Pro-Rector	
Registrar	
Sr Dy Registrar (P.F.)	
Dy Registrar (P.F.)	
Asst Registrar (P.F.)	
Asst Registrar (P.F.)	
Supervisor / Head Clk	
Date	10/10/23

→ Pl circulate as per
remarks of Pro-Rector. ✓
Sajjad

GOVERNMENT OF PAKISTAN
CABINET SECRETARIAT
CABINET DIVISION
(NTISB)

PA 28/9 -107

No. 1-5/2003 (NTISB-II)

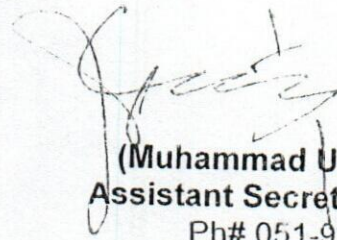
Islamabad, the 20 September, 2023

Subject: - Cyber Security Advisory – Latest Android Patches/Updates/Fixing Zero Day Vulnerabilities (Advisory No. 55)

Recently, Google has applied patches to Android OS versions 11, 12 and 13 via Google Play Protect service, fixing 32x flaws including one zero-day vulnerability; CVE-2023-35674 (privilege escalation flaw affecting android framework further leading to remote code execution). These updates are floated only for android devices running OS version 11 and above.

2. Above in view, all android OS users are advised to enable Google Play Protect service to receive notifications for latest updates. Also, devices running android OS version 10 and below are advised to update to the latest versions (11 or above)

3. Kindly disseminate the above information to all concerned in your organizations, all attached/affiliated departments and ensure necessary protective measures.


(Muhammad Usman Tariq)
Assistant Secretary-II (NTISB)
Ph# 051-9204560

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

Copy to: -

1. Secretary to the Prime Minister, Prime Minister Secretariat, Islamabad
2. Secretary to the President, Aiwan-e-Sadar, Islamabad
3. Cabinet Secretary, Cabinet Division, Islamabad
4. Additional Secretary-III, Cabinet Division, Islamabad
5. Director General (Tech), Dte Gen, ISI Islamabad
6. Director (IT), Cabinet Division, Islamabad

for...
28/9
28-9-23
AS

SECRETARY MOST
Dy. No. 3640

Additional Secretary MOST
Dy. No. 2866
Date: 29/9/23

957-JE
28-9-2023

Dy. No. 51
Date: 28.9.2023

-108-

GOVERNMENT OF PAKISTAN
CABINET SECRETARIAT
CABINET DIVISION
(NTISB)

No. 1-5/2003 (NTISB-II)

Islamabad, the 20 September, 2023

Subject: - Cyber Security Advisory – Apple iPhones Targeted with Blast Pass Exploit to Deploy Pegasus Spyware (Advisory No. 56)

Context. Reportedly, Apple iPhone users are being targeted by NSO Group's nefarious Spyware i.e. Pegasus. The exploitation process is instigated through iMessage feature (CVE-2023-41061 and CVE-2023-41064) for deployment of Blast Pass (zero day and zero click malware).

2. **Blast Pass Exploit.** Blast Pass is capable of infecting OS latest versions (16.6) without user interaction. In this regard, Apple has issued remedial advisory for iPhone users. Apple has also generated alerts to inform its users for being targeted by NSO Pegasus spyware or likely targeted by state-sponsored attackers. Apple users are urged to follow safety steps mentioned at para-3 to prevent against Blast Pass Pegasus exploit and other prevalent cyber-attacks.

3. **Specific Safety Steps to Blast Pass Exploit**

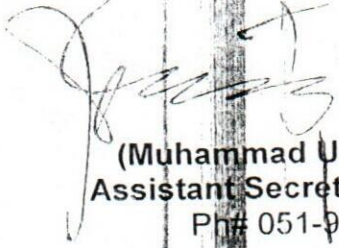
- a. Immediately upgrade to iOS latest version (16.6.1 or above) which covers majority of security updates related to ongoing attacks.
- b. Enable lockdown mode (optional; extreme protection mode) to block Blast Pass attack.
- c. Disable iMessage feature available in iPhones.

4. **Generic Security Steps for Apple Users**

- a. Protect devices with strong passcodes and use two factor authentications on Apple ID.
- b. Install apps from official Apple Store only to avoid malware/infection.
- c. Use anonymity-based solutions (over internet while surfing) and mask identity of key appointment holders/individuals.
- d. Always disable location from Apple devices.

- 109,
- e. Subscribe to Apple's security bulletins, threat notifications and auto OS update features.
 - f. Strictly avoid using phones at sensitive locations/meetings.

3. Kindly disseminate the above information to all concerned in your organizations, all attached/affiliated departments and ensure necessary protective measures.


(Muhammad Usman Tariq)
Assistant Secretary-II (NTISB)
Ph# 051-9204560

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

Copy to: -

1. Secretary to the Prime Minister, Prime Minister Secretariat, Islamabad
2. Secretary to the President, Aiwan-e-Sadar, Islamabad
3. Cabinet Secretary, Cabinet Division, Islamabad
4. Additional Secretary-III, Cabinet Division, Islamabad
5. Director General (Tech), Dte Gen, ISI Islamabad
6. Director (IT), Cabinet Division, Islamabad

110

GOVERNMENT OF PAKISTAN
CABINET SECRETARIAT
CABINET DIVISION
(NTISB)

No. 1-5/2003 (NTISB-II)

Islamabad, the 21 September, 2023

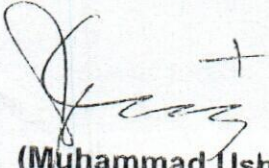
Subject: - Cyber Security Advisory - Adobe Acrobat Reader Critical Vulnerabilities Patch Available (Advisory No. 58)

Adobe has recently released security updates for Adobe Acrobat Reader software versions to fix critical zero-day vulnerability (CVE-2023-26369; Remote Code Execution Vulnerability) running on Apple and Microsoft devices. Non-patching of the updates can be exploited by threat actors to execute malicious code. However, exploitation requires user interaction (user must open a malicious file sent via phishing attack). Affected products include:

- a. Adobe Acrobat DC versions 23.003.20284 (and earlier)
- b. Adobe Acrobat Reader DC versions 23.003.20284 (and earlier)
- c. Adobe Acrobat 2020 versions 20.005.30516 (earlier) for Mac & 20.005.30514 (and earlier) for Windows
- d. Adobe Acrobat Reader 2020 versions 20.005.30516 (and earlier) for Mac & 20.005.30514 (and earlier) for Windows

2. Users are advised to update their software to the latest versions according to devices' compatibility from official stores; Adobe Acrobat Reader versions 23.006.20320/20.005.30524; dated 13th September, 203 (or above).

3. Kindly disseminate the above information to all concerned in your organizations, all attached/affiliated departments and ensure necessary protective measures.


(Muhammad Usman Tariq)
Assistant Secretary-II (NTISB)
Ph# 051-9204560

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

Copy to: -

1. Principal Secretary to the PM, Prime Minister's Secretariat, Islamabad
2. Secretary to the President, Aiwan-e-Sadar, Islamabad
3. Cabinet Secretary, Cabinet Division, Islamabad
4. Additional Secretary-III, Cabinet Division, Islamabad
5. Director General (Tech), Dte Gen, ISI Islamabad
6. Director (IT), Cabinet Division, Islamabad

GOVERNMENT OF PAKISTAN
CABINET SECRETARIAT
CABINET DIVISION
(NTISB)

No. 1-5/2003 (NTISB-II)


Islamabad, the 21 September, 2023

Subject: - Cyber Security Advisory - Google Chrome Version Update (Advisory No. 59)

Google has released security patch for its Chrome Browser in its latest software version to fix critical vulnerability CVE-2023-4863; buffer overflow in WebP Code Library. Google Chrome updated version 116.05845.187 for Mac and Linux and version 116.0.5845.187.188 is available for Windows systems. The flaw, if exploited, may lead to DDoS attack and Remote Code Execution (RCE) via HTML pages.

2. Above in view, Chrome users are recommended to update to the latest version from official stores.

3. Kindly disseminate the above information to all concerned in your organizations, all attached/affiliated departments and ensure necessary protective measures.


(Muhammad Usman Tariq)
Assistant Secretary-II (NTISB)
Ph# 051-9204560

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

Copy to: -

1. Principal Secretary to the Prime Minister, Prime Minister's Secretariat, Islamabad
2. Secretary to the President, Aiwan-e-Sadar, Islamabad
3. Cabinet Secretary, Cabinet Division, Islamabad
4. Additional Secretary-III, Cabinet Division, Islamabad
5. Director General (Tech), Dte Gen, ISI Islamabad
6. Director (IT), Cabinet Division, Islamabad