Government of Pakistan
Ministry of Aviation
*****

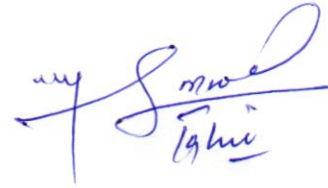F. No. 1(2)/2023-IT-NA   Islamabad, the 22ᵗʰ August, 2024

MEMORANDUM

Subject: -   **CYBER SECURITY ADVISORY – Google Chrome Security Update
(Advisory No.15.
CYBER SECURITY ADVISORY – Windows Outage affecting Version 10 and
11 Globally (Advisory No.16)
CYBER SECURITY ADVISORY – Konfety Group Targets Android Users
with Evil Twin Malicious Play Store Aps (Advisory No. 17)
CYBER SECURITY ADVISORY – Prevention against Cyber-Attack on the
Event of National Days (Advisory No.18)**

Please find enclosed a copy of Cabinet Division's Memorandum No. 1-5/2003/24 (NTISB-II), on the subject cited above for compliance of directions therein.

Encl: As above

(Hafiz Tahir Mahmood)
Network Administrator
Tel: 051-9203217

i.   Director General,
        Civil Aviation Authority, HQ
        Karachi

ii.   Adeel Yousfani
        PIA IT Building Ground Floor Network Hall
        Karachi.

iii.   Director General,
        Airports Security Force, HQ
        Karachi

iv.   Director General,
        Pakistan Meteorological Department, Sector H-8/2
        Islamabad

GOVERNMENT OF PAKISTAN
CABINET SECRETARIAT
CABINET DIVISION
(NTISB)

F. No. 1-5/2003/24(NTISB-II)　　　　　　　Islamabad, the 30th July, 2024

Subject:　**Cyber Security Advisory - Google Chrome Security Update (Advisory No. 15)**
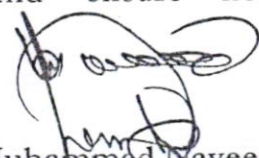
　　　　Introduction.　Google has released Chrome browser version 126 with security updates to address 10 vulnerabilities.

2.　　　**Vulnerability Details.**　Majority of the vulnerabilities are high-severity memory issues potentially leading to Sandbox Escapes and Remote Code Execution. Fixes include flaws in V8's Implementation, Type Confusion and Use-After-Free bugs in Screen Capture, Media Stream, Audio and Navigation. Google also addressed Race Condition in DevTools and an Out-of-Bound memory access in V8. No exploits in the wild are reported but users are urged to update promptly.

3.　　　**Recommendations.**　To safeguard against Chrome vulnerabilities, users are advised to ensure that Google Chrome browser is updated to following versions (by navigating to Setting>About Chrome and Relaunching the browser):

　　　a.　Version 126.0.6478.182 or later on Windows/Linux
　　　b.　Version 126.0.6478.183 or later on macOS
　　　c.　Version 126.0.6478.186 or later on Android

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

　　　　　　　　　　　　　　　　　　　　　(Muhammad Naveed)
　　　　　　　　　　　　　　　　　　　　Deputy Secretary (NTISB)
　　　　　　　　　　　　　　　　　　　　Ph# 051-9204560

All Secretaries of Ministries/Divisions of the Federal Government and Chief Secretaries of the Provincial Governments
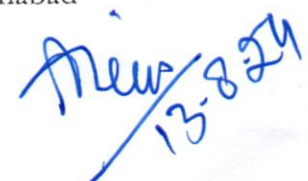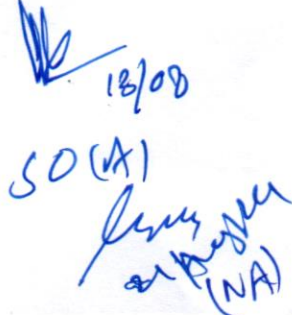
Copy to:
1. Principal Secretary to the PM, Prime Minister's Secretariat, Islamabad
2. Secretary to the President, Aiwan-e-Sadar, Islamabad
3. Cabinet Secretary, Cabinet Division, Islamabad
4. Additional Secretary-III, Cabinet Division, Islamabad
5. Director General (Tech), Dte Gen, ISI Islamabad
6. Director (IT), Cabinet Division, Islamabad

GOVERNMENT OF PAKISTAN
CABINET SECRETARIAT
CABINET DIVISION
(NTISB)

Islamabad, the 5th August, 2024

F. No. 1-5/2003/24(NTISB-II)

Subject: <u>Cyber Security Advisory – Windows Outage Affecting Version 10 and 11 Globally (Advisory No. 16)</u>

<u>Introduction</u>. A recent update to CrowdStrike's Falcon sensor has caused significant disruptions for Windows 10 and 11 users globally, leading to Blue Screen of Death (BSOD) loops and rendering systems inoperable. Users report repeated BSODs with the error message DRIVER_OVERRAN_STACK_BUFFER, preventing normal system boot and operation.

2. <u>Incident Details</u>. The impact has been particularly severe to large enterprises (banks, airlines, hospitals, broadcasters etc.), with some organizations reporting thousands of affected devices, including critical production servers.

3. <u>Recommendations</u>. Above in view, to safeguard against Windows outage issue, users are advised to ensure backup and high availability of critical services/data/systems as a contingency measure. Moreover, in order to specifically resolve above mentioned issue, users/administrators are advised to perform following steps:

   a. Boot windows into safe mode or the windows recovery environment
   b. Navigate to this directory: C:\Window\System32\Drivers\CrowdStirke
   c. Locate the file matching C-00000291*.sys and delete this file
   d. Finally, boot the windows normally after removing above mentioned file
   e. Crowdstrike fix may be applied on test environment and on successful test-run (24 hours) may be deployed on production systems

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

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

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

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)
****

F. No. 1-5/2003/24(NTISB-II)　　　　　　　　Islamabad, the 12 August, 2024

Subject: <u>Cyber Security Advisory – Konfety Group Targets Android Users with Evil Twin Malicious Play Store Apps (Advisory No. 17)</u>

　　　　Introduction.　　Recently, Google Play Store identified and thwarted an active malicious campaign targeting Android users globally. Collectively named as Konfety Apps; this campaign used 250+ Decoy Evil Twin android applications (**Annex - A**). The malicious activity is allegedly conducted by the Russian Konfety cybercrime group having ulterior motives primarily backed by monetary gains using advertisement fraud.

2.　　**Modus Operandi.**　　Attackers use advertising campaigns to promote modified APK and redirects users to download malicious apps. Konfety malware involves a dropper APK that further loads an obfuscated stager and back doored SDK, making it highly evasive hence difficult to detect. Further, the decoy twin apps used by attackers appear harmless while Evil Twin mimics them to commit ad fraud, install payloads, second stage malwares and code injection etc.

3.　　**Mitigation.**　　Although Google has removed Konfety apps from its Play Store, however, if any of the attached malicious Konfety apps found installed on smart phones, following remedial measures may be opted:

　　a.　Immediately uninstall specific Konfety app.

　　b.　Perform a factory reset.

　　c.　Take a backup of personal media files (excluding device/system apps).

　　d.　Restrict unnecessary apps permission and set to while using App only.

　　e.　Download and install software only from official app stores like Play Store or the IOS App Store.

　　f.　Keep your smart phone, OS and apps updated.

　　g.　Regularly check the smart devices/Wi-Fi data usage of apps installed on smart devices.

　　h.　Use a reputed anti-virus and internet security software package on your smart devices.

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

(Muhammad Usman Tariq)
Assistant Secretary (NTISB-II)
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

LIST OF KONFETY MALICIOUS EVIL TWIN DECOY APPS
(Already Removed by Google Play Store)

Ser	App Name	Ser	App Name
1.	Best Status	2.	Learn English Urdu
3.	Akbar	4.	Galaxy Fighter
5.	Dream Head Soccer	6.	Drive me
7.	Sweet Candy Cream Rain	8.	Double Co
9.	Block Puzzle	10.	Goddess Photo
11.	Endless Airplane	12.	Dict En lt Free
13.	Modern Snake	14.	Santa Stuck
15.	Car Crash	16.	Street Fight
17.	Draw	18.	Tourism
19.	Spin Tunnel	20.	Jewel Puzzle New
21.	X Racer	22.	Head Soccer
23.	Skate Surfers	24.	Tunnel
25.	Tuneonn Lal	26.	Space Craft
27.	Tennis Ball Bounce	28.	Shark Hunter Hungry Fish
29.	Viking Saga	30.	Bouncy Ball
31.	Indian Border Animal	32.	Falling Blocks
33.	Downhill Bus Racing	34.	Survival Secret Agent Prison Mafia
35.	Football Cup	36.	Eye Color Editor
37.	Fruit Splash	38.	Basketball
39.	Car Chase	40.	GTi Drag Desert
41.	Max Parking	42.	Jump Ninja
43.	Tank Battle Games Free	44.	Words Play
45.	Ball Hop	46.	MP3 Cutter
47.	Monster Defense	48.	Insta Frame Pic Collage

49.	Proverbs and Sayings	50.	Swing Thru
51.	Bounce Ball 2	52.	Dvng Doggo
53.	Piano Balls	54.	High Dive
55.	Latest Punjabi Songs	56.	Tuneom Dohe
57.	Tuneonn Horror	58.	Animal Dash King
59.	Offroad Racing	60.	Tuneonn Yoga
61.	Tuneonn Jokes	62.	Personal Voice Judge
63.	Draw My Story	64.	Smart Quiz Price
65.	Zombie Apocalypse	66.	Self-Study Yoga
67.	Candy Heroes Mania	68.	Drift Tuner 2019
69.	Tuneonn Ayurveda	70.	Ni Mobile
71.	Soccer Ping	72.	Caesar Empire
73.	Color Jump	74.	Flight Sim 3D Pilot
75.	Fruit Sweet Blast	76.	Big Farm
77.	Myth Puzzle	78.	Four Pics One Word
79.	Sniper War Survival	80.	Flash Cards English
81.	R Drift	82.	Border Line
83.	Boom Rocket	84.	Aptitude Test
85.	Life Quote	86.	Fatty Ninja
87.	Destiny Photo Mixer	88.	English Status And Message
89.	English Stories	90.	Mind Quiz Brain Out
91.	UPSSSC Exam	92.	Deep Sea Adventure
93.	Bike Trail Stunt Master Racing Games	94.	Qiu Qiu Jstzs
95.	Umbrella Down	96.	Cook Book
97.	Pets Animals	98.	Back Hand Spring
99.	Furious Speed Car Stunt	100.	Fruit Juice
101.	Moto Racing Bike Stunt Traffic Racer	102.	Mao Miecz
103.	Indian Mountain Jeep Drive	104.	G Ball

105.	Truck Bike Racing	106.	Congratulation
107.	Ludo Star Master	108.	Ludo Legend
109.	Colo Monopoly	110.	Gravity Pipes
111.	Stic Balls	112.	Nature Puzzle
113.	Military Suit Photo Montage	114.	Subway Surf
115.	Runner Subway	116.	Tip King
117.	Pac Monoid	118.	Love Que
119.	M Food	120.	Dino Bomb
121.	Cat Run	122.	Tamil
123.	Chess Opening	124.	Space Ship
125.	Jewel Deluxe	126.	Dict En Ru Free
127.	Devil Fighter	128.	Reasoning
129.	Apple Shooter Game	130.	Bhakti Rings
131.	Fight Ord	132.	Wrapping Bubbling
133.	Test Inteligencia	134.	Enigmas
135.	Status Katta	136.	Billiard Club Deluxe
137.	Critical Strikes	138.	Devinettes
139.	Speed Car Bump Challenge	140.	GTR Redline Racing
141.	Cook From Bis	142.	Racing Girl
143.	Candy Splash	144.	Meme Katta
145.	Handled Spinner	146.	Yanggedw
147.	Racing Stunt Man	148.	Blind Zombie
149.	Pr Call Ghost	150.	Caesar Empire
151.	Dragon Hunter	152.	Retro Drag
153.	Crazy Bike Racing Simulator	154.	Kawaypk
155.	Apk Share For You	156.	Ma Mam Nq01
157.	Race and Kill	158.	Brain Ball Bash
159.	Oil Train Transporter	160.	Cartoon Quiz

161.	Candy Land	162.	Video Media Mp3 Cutter
163.	Cooking Fever Craze Expert Madness	164.	Snow Queen 2 Bird Weasel
165.	Calculator Talks	166.	Double Corks
167.	Cube Jump	168.	TSR
169.	Romantic Bells	170.	Aqua Fish
171.	Tractor Offroad	174.	Tap Soccer
173.	Flappy Bee	174.	Bistro Cook
175.	Selfi Cam Beauty	176.	Waheguru Ji Tone Mp3
177.	Acertijo	178.	Hindi Grammar
179.	Japan Race	180.	Buyaocc2
181.	Kick It	182.	Gongfu Hcrwz
183.	Missiles	184.	Huochai Rjtzz
185.	Sticky Mn	186.	Fk Xrty
187.	High War Racer	188.	Fighter Two Players
189.	Real Drift	190.	Shark Hunter Hungry Fish 2
191.	Star Stell Story	192.	Learn English Tenses In Urdu
193.	Heavy Bike Racer	194.	Dict English Synonyms Free
195.	Soccer Kicks Penalty Shootout	196.	Pr Call Burger
197.	Angry Bunnies	198.	Diving Doggy
199.	Tonne For Arabs	200.	Rubicon Car Stunts
201.	Drawing the Path	202.	Adriver Jyeghz
203.	Train Simulator	204.	M Scary
205.	Jump One Jump	206.	Dubgeon
207.	Zigzag Highway	208.	English Flash Card Learn Word
209.	Jump Bump	210.	Jiroutr
211.	Old Movies	212.	Maze
213.	Marathi	214.	Dict En El Free
215.	Trump Talk	216.	Pet Parkour

217.	Hindi Status	218.	Plane Flight Pilot Landing Sim
219.	Window Photo Editor	220.	Play Mini World
221.	Fortress Defense	222.	Tuneonn Love Stories
223.	Monte Cristo Link To 8 Puzzle	224.	Waheguru Ji Tones
225.	Tuneonn Health Tips	226.	Xiao Jie Jahz
227.	Car Wash	228.	Zombieland
229.	Tuneonn Vastu	230.	Adriver Ezjdzz
231.	Latest Arabic Ring	232.	Chess Game
233.	Conversation	234.	Vid Fake Scary Mo
235.	Snr Near	236.	Mp3 Cutter
237.	Puzzle Classic	238.	English Toefl Learn Word
239.	Slime	240.	Dict En Hi Free
241.	Picture Game	242.	Nbzh
243.	Fallin Ball	244.	English Audio Story
245.	Flib Bottle	246.	Stickman Backflip Pro
247.	Coloring App	248.	Slime Wallpapers
249.	TSR	250.	Hidden Object
251.	Maths	252.	Dict French Free
253.	Tuneonn Hindi Stories	254.	Drawing The Path
255.	Swings	256.	Snow Queen Bird Weasel

GOVERNMENT OF PAKISTAN
CABINET SECRETARIAT
CABINET DIVISION
(NTISB)
****

F. No. 1-5/2003/24(NTISB-II)

Islamabad, the 12 August, 2024

Subject: **Cyber Security Advisory - Prevention against Cyber-Attacks on the Event of National Days (Advisory No. 18)**

It has generally been observed that hostile elements tend to sabotage National Days of Pakistan by disrupting IT services of critical information infrastructure (CII), Government Ministries and departments. On the occasion of Independence Day (14 August, 2024), IT/OT services disruption attempts by hostile elements cannot be ruled out.

2.   In addition, hostile elements/state sponsored malicious actors typically target IT infrastructure/websites of Defence sector and sensitive installations to tarnish the 'global' image of Pakistan.

3.   It is likely that hostile elements may launch cyberattacks on CII on National Days (14 Aug and 6 Sep 2024).

4.   Above in view, Cyber Security best practices are attached (**Annex-A**) to sensitize CII regulators, stakeholders, IT/website administrators and service providers to take additional security precautions (such as sustenance of internet backhaul against DDoS attack, web server hardening, traffic/integrity monitoring etc.) to avoid possible service disruption, website defacement and hacking attempts.

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

(Muhammad Usman Tariq)
Assistant Secretary (NTISB-II)
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

CYBER SECURITY BEST PRACTICES FOR PROTECTION OF IT INFRASTRUCTURE

Guidelines for IT/Web Admins

1. Upgrade OS and webservers to latest version.

2. Website admin panel should only be Accessible via white-listed IPs.

3. Defend the website against SQL injection attacks by using input validation technique.

4. Complete analysis and penetration testing of application be carried out to identify potential threats.

5. Complete website be deployed on inland servers including database and web infrastructure.

6. HTTPS protocol be used for communication between client web server.

7. Application and database be installed on different machines with proper security hardening.

8. Sensitive data be stored in encrypted form with no direct public access.

9. DB user privileges be minimized and limited access be granted inside programming code.

10. Proper security hardening of endpoints and servers be performed and no unnecessary ports and applications be used.

11. Updated Antivirus tools/ Firewalls be used on both endpoints and servers to safeguard from potential threats.

12. Enforce a strong password policy.

13. Remote management services like RDP and SSH must be disabled in production environment.

14. Deploy Web Application Firewalls (WAF) for protection against web attacks.

15. Employ secure coding practices such as parameterized queries, proper input sanitization and validation to remove malicious scripts.

16. Keep system and network devices up-to-date.

17. Log retention policy must be devised for at least 3x months on separate device for attacker's reconnaissance.

Guidelines for Email Security

1. ### Use Strong Passwords

    a. To ensure email security, always use strong passwords by employing combination of alphanumeric, Special characters, upper and lower case letter.

    b. Avoid using general and easily guessable passwords e.g. DOB, own/family names, vehicle registration number etc.

    c. Regularly change passwords.

2. ### Avoid Email ID Exposure

    a. Avoid sharing email ID with unknown persons.

    b. Always confirm the identity of the individual to/ from whom email is being sent/received.

    c. Avoid providing personal details in suspicious internet campaigns.

    d. Never use official email for private communication. Always use separate email IDs for personal and official correspondence.

    e. Never configure/ use official email on mobile phones.

3. ### Be Aware of Phishing Attacks

    a. Never open email attachments from unknown sources/senders.

    b. If an email seems suspicious, just ignore it; even don't try to unsubscribe it by clicking unsubscribe link as it may allow hacker to access your emails data.

    c. Never open any attachment without anti-virus scan.

    d. If any suspicious email is received immediately consult IT Administrator of your, organization.

4. ### Always Send Password Protected Documents

    a. All email attachments sent must be encrypted with password.

    b. Password must be communicated through a separate channel such as SMS, Call or WhatsApp message.

    c. Delete password from the sending channel (SMS, WhatsApp etc) once received by the receiving party.

5. ### Use Two Factor Authentication

    a. In addition to strong passwords, also use two factor authentication e.g. OTP via call/ message, password reenter mechanism-etc.

    b. Never share your One Time Password (OTP) with anyone.

6. <u>Use Well Reputed and Licensed Anti-Virus</u>

   a. Endpoint (computer system or laptop) on which official email/data is being accessed/sent must be secured through reputed, licensed and updated antivirus/anti-malware solution.

   b. Always keep system Firewalls activated and updated.

7. **Use Robust Paid Anti-Spam Filters**

   a. Use reputed Spam Filters.

   b. Do not rely on Google/Yahoo's Spam Filters as email attackers have become much sophisticated.

8. **Avoid Storing Data on Cloud Storage**

   a. Never Store personal and official data on cloud storage.

   b. Avoid using online document converting tools (Word to PDF etc) with cloud based data storage technology.

9. **Guidelines for Social Media Platforms, GSM and PDF Scanner**. Few guidelines (but not limited to) are as under:

   a. Do not share official documents via WhatsApp, Telegram, Messenger and other so called end-to-end encrypted messaging apps/secret chatting applications as their servers are hosted outside Pakistan.

   b. Do not use online PDF Scanner apps., Only scan secret documents via official hardened scanners.

   c. Do not discuss secret official matters on call/SMS/landline/GSM WhatsApp etc. Use officially dedicated communication numbers.

   d. Never store secret official documents in personal mobiles, PC.

   e. Do not store secret official documents in online systems. Always delete data after usage.

   f. Avoid using free and lucrative apps as majority of them steal data from PC and mobile phones.

   g. Do not use cracked versions of software. Always install paid software from official support and store.

   h. Ensure hardening of all online and offline official system.

10. **General Guidelines**

   a.   Public WiFi is more susceptible to attack as compared to private WiFi.

   b.   Public WiFi Administrator might be monitoring network traffic and data sent online via internet packets.

   c.   Passwords may be stored by network Administrator. Therefore, avoid using public WiFi for accessing personal/ official email.

   d.   Regularly check and apply security updates.

****