



R.O. 334

14.2.2022

No.E&A(Agri)6-334/2022
GOVERNMENT OF THE PUNJAB
AGRICULTURE DEPARTMENT

Dated Lahore, the 31st January, 2022

To

1. The Director General Agriculture (Ext. & A.R.), Punjab, Lahore.
2. The Director General Agriculture (Field) Punjab, Lahore.
3. The Chief Scientist Agriculture (Research), Ayub Agricultural Research Institute, Faisalabad.
4. The Director General Agriculture (WM), Punjab, Lahore.
5. The Director General, PW & QC of Pesticides, Punjab, Lahore.
6. The Director General, Soil Survey of Punjab, Multan Road, Lahore.
7. The Director of Agricultural Information, Punjab, Lahore.
8. The Director of Agriculture, Crop Reporting Service, Punjab, Lahore.
9. The Chief, P&E Cell, Agriculture Department, Lahore.
10. The Chief (WTO), Agriculture Department, Davis Road, Lahore.
11. The Director of Agriculture (E&M), Punjab, Lahore.
12. The Chief Coordinator, RAEDC, Vehari.
13. The Director of Floriculture (T&R), Punjab, Lahore.
14. The Director, Punjab Institute of Agriculture Marketing (PIAM), Lahore.
15. The Managing Director, Punjab Seed Corporation, Lahore.
16. The Registrar, University of Agriculture, Faisalabad.
17. The Chief Executive, Punjab Agricultural Research Board, Lahore.
18. The Registrar, Arid University of Agriculture, Rawalpindi.
19. The Director, Market Committee Provincial Fund Board, Lahore.
20. The Registrar, Muhammad Nawaz Sharif University of Agriculture, Multan.
21. The Chief Technical Advisor, Agriculture Delivery Unit (ADU), Lahore.
22. The Secretary Agriculture Commission, Lahore.
23. The Chief, Sugarcane Research & Development Board, Faisalabad

Subject:- **ADVISORY – PREVENTION AGAINST INDIA ORIENTED
OFFLINE MAPS MOBILE APPLICATION-DEESHA (ADVISORY
NO.94)**

I am directed to refer to the subject noted above and enclose herewith a copy of letter No.SO(FG)3-72/2021 (Vol-I), dated 17.01.2022 alongwith its enclosure received from Section Officer (FG-I), Government of the Punjab, S&GAD is forwarded for information and strict compliance.

SECTION OFFICER (GENERAL)
Ph. No.99210505

DR (14/2)
14/2
14/2



No.S0(FC)3 72/2021 (Vol-I)
GOVERNMENT OF THE PUNJAB
SERVICE & GENERAL ADMINISTRATION
DEPARTMENT
(I&C WING)

Dated Lahore, the 17th January 2022

32

To

SS Agri	
AS (A)	✓
AS (P)	
AS (TF)	
Chief P&EC	
PO	
PS	

- The Senior Member, Board of Revenue, Punjab
- The Chairman, P&D Board, Punjab.
- The Additional Chief Secretary, Punjab.
- All the Administrative Secretaries, Government of the Punjab.
- The Inspector General of Police, Punjab.
- All the Divisional Commissioners in Punjab.
- The Chairman, Punjab Information Technology Board.

Diary No. 01063
Date 24-1-22
Agriculture Deptt.
Civil Secretariate Lhr.

P.A. to A.S. Admn

Diary No. 287

Date 25-1-22

01-1

Subject: ADVISORY -PREVENTION AGAINST INDIA ORIENTED OFFLINE MAPS MOBILE APPLICATION-DEESHA (ADVISORY NO.94).

Re circulate

Kindly refer to the subject cited above and find enclosed herewith a copy

of letter No.1-5/2003(NTISB-II)/24 dated 11.01.2022 received from Assistant Secretary-II (NTISB), Government of Pakistan, Cabinet Secretariat, National Telecom and Information Technology Security Board (NTISB), Islamabad for necessary action and further distribution to field formation for compliance, please.

S/O (Agri)
26/11

(SECTION OFFICER (FG-I))

P.L. circulate
26/11

- Assistant Secretary-II (NTISB), Government of Pakistan, Cabinet Secretariat, National Telecom and Information Technology Security Board (NTISB), Islamabad w/r/t his letter referred above.
- FS to Secretary (I&C), S&GAD.

SA

DS (A-I)

Diary No. 202

Date 26-1-22

E & A Section
Diary No. 127
Date 27-01-22
Govt. of the Punjab
Agri. Deptt.

26/11/2022

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

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

Islamabad 11 January 2022

Subject: Advisory - Prevention against Indian Oriented Offline Maps Mobile Application - Deesha (Advisory No.94)

1. Introduction.

Recently, it has been observed that an Indian origin 3rd party Android navigational application "Deesha" is being used for offline road navigation. The application is not available on Google Play store and may be downloaded from 3rd party servers. Users feedback of the application is quite positive, hence, its large scale usage in future cannot be ruled out.

2. Features - Deesha Application.

The application automatically gets access to host system, data store, SMS read and location permission without prior knowledge of the users. Additional features of the application include; displaying location in Indian Grid System with accuracy, navigation to save way points, photo geotagging, location sharing, map view with panning and zooming option and displaying device way points. Computation of location is independent of availability of internet / mobile network. As Deesha is an Indian 3rd party app, hence, under command organizations / users may be instructed to refrain from its use. Few best practices / recommendations to be adhered to while downloading / using mobile applications are mentioned at Para 3.

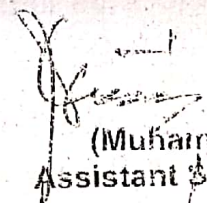
3. Best Practices / Recommendations for Mobile Application Usage

- a. **Block all applications installs from unknown sources**, these options are disabled in Android by default and it should stay that way.
- b. Only install application form official App Stores / **Google Play Store**.
- c. **Google Play protect** (Android built in Anti Malware) **must not be switched off** in any case. It detects suspicious looking apps in your mobile device based on their behavior and generates alerts for user.
- d. **Do not click on links that promise unusual features or functionalities** such as "WhatsApp offers of free Airline Tickets" are usually just an attempt to steal your personal data. The same applies to phishing including texts from friends containing suspicious URLs.
- e. Before installing any application, **user must read its privacy policy explaining what data it is collecting form users and with whom it is**

- f. It is strongly recommended to all users to ensure keeping their communication app up-to-date from their respective App Stores. Do not ignore updates from apps installed on your device.
 - g. Regularly Update Mobile Operating System whenever updates are available.
 - h. Use of mobile Antivirus in order to prevent any danger that may affect your Personal data on device.
 - i. Carefully consider what information you want to store on the device, remember that with enough time, sophistication and access to the device, an attacker can obtain your stored information.
 - j. Be careful when using social networking apps; these apps may reveal personal information to unintended parties. Be especially careful when using services that track your location.
4. Disseminate the same to attached / affiliated, Departments and Branches forwarded for necessary action, please.

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

asntisb2@cabinet.gov.pk


 (Muhammad Usman)
 Assistant Secretary-II (NTISB)
 Ph: 051-920453

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

Copy to: -

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



No.E&A(Agri)6-334/2022
GOVERNMENT OF THE PUNJAB
AGRICULTURE DEPARTMENT

Ro.33
14.2.20

Dated Lahore, the 31st January, 2022

To

1. The Director General Agriculture (Ext. & A.R.), Punjab, Lahore.
2. The Director General Agriculture (Field) Punjab, Lahore.
3. The Chief Scientist Agriculture (Research), Ayub Agricultural Research Institute, Faisalabad.
4. The Director General Agriculture (WM), Punjab, Lahore.
5. The Director General, PW & QC of Pesticides, Punjab, Lahore.
6. The Director General, Soil Survey of Punjab, Multan Road, Lahore.
7. The Director of Agricultural Information, Punjab, Lahore.
8. The Director of Agriculture, Crop Reporting Service, Punjab, Lahore.
9. The Chief, P&E Cell, Agriculture Department, Lahore.
10. The Chief (WTO), Agriculture Department, Davis Road, Lahore.
11. The Director of Agriculture (E&M), Punjab, Lahore.
12. The Chief Coordinator, RAEDC, Vehari.
13. The Director of Floriculture (T&R), Punjab, Lahore.
14. The Director, Punjab Institute of Agriculture Marketing (PIAM), Lahore.
15. The Managing Director, Punjab Seed Corporation, Lahore.
16. The Registrar, University of Agriculture, Faisalabad.
17. The Chief Executive, Punjab Agricultural Research Board, Lahore.
18. The Registrar, Arid University of Agriculture, Rawalpindi.
19. The Director, Market Committee Provincial Fund Board, Lahore.
20. The Registrar, Muhammad Nawaz Sharif University of Agriculture, Multan.
21. The Chief Technical Advisor, Agriculture Delivery Unit (ADU), Lahore.
22. The Secretary Agriculture Commission, Lahore.
23. The Chief, Sugarcane Research & Development Board, Faisalabad

Subject:- **CYBER SECURITY ADVISORY-VULNERABLE NHA WEBSITE AND MOTORWAY MOBILE APPLICATION (ADVISORY NO.93)**

I am directed to refer to the subject noted above and enclose herewith a copy of letter No.SO(FG)3-72/2021 (Vol-I), dated 17.01.2022 alongwith its enclosure received from Section Officer (FG-I), Government of the Punjab, S&GAD is forwarded for information and strict compliance.

[Handwritten signature]

14/2/2022

[Handwritten signature]

SECTION OFFICER (GENERAL)
Ph. No.99210505

DR (G/I)
[Handwritten signature]

28

TOP PRIORITY



No.SO(FG)3-72/2021 (Vol-I)
GOVERNMENT OF THE PUNJAB
SERVICE & GENERAL ADMINISTRATION
DEPARTMENT
(I&C WING)

Dated Lahore, the 25th January 2022

To

1. The Senior Member, Board of Revenue, Punjab
2. The Chairman, P&D Board, Punjab.
3. The Additional Chief Secretary, Punjab.
4. All the Administrative Secretaries, Government of the Punjab.
5. The Inspector General of Police, Punjab.
6. All the Divisional Commissioners in Punjab.
7. The Chairman, Punjab Information Technology Board.

Diary No. 01131
Date 25-1-22
Agriculture Deptt.
Civil Secretariate Lhr.

SS Agri	
AS (A)	✓
AS (P)	
AS (IF)	
Chief P&EC	
PD	
PS	

Subject:- CYBER SECURITY ADVISORY-VULNERABLE NHA WEBSITE AND MOTORWAY MOBILE APPLICATION (ADVISORY NO.03)

Kindly refer to the subject cited above and find enclosed herewith a copy of letter No.1-5/2003(NTISB-II) dated 11.01.2022 received from Assistant Secretary-II (NTISB), Government of Pakistan, Cabinet Secretariat, National Telecom and Information Technology Security Board (NTISB), Islamabad for necessary action and further distribution to field formation for compliance, please.

(SECTION OFFICER (FG-I))

297
25-1-22
Dr-1 c.c.:

1. Assistant Secretary-II (NTISB), Government of Pakistan, Cabinet Secretariat, National Telecom and Information Technology Security Board (NTISB), Islamabad w/r/t his letter referred above.
2. PS to Secretary (I&C), S&GAD.

re circulate

SO(G)

DS (A-I)

Diary No. 209

Date 26-1-22

re circulate
Jull

26/1

asm
1/1/2022

SA

E & A Section
Diary No. 120
Date 27.01.22
Govt. of the Punjab
Agri. Deptt.

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

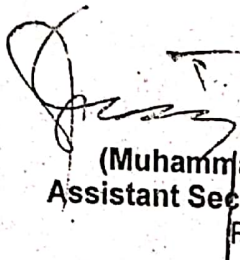
No. 1-5/2003 (NTISB-II)

Islamabad 11 January 2022

Subject:- Cyber Security Advisory – Vulnerable NHA website and Motorway
Mobile Application (Advisory No. 93)

1. It has been observed that National Highway Authority's (NHA) website (nha.gov.pk) and Motorway's M-Tag mobile application onenetwork.pk are vulnerable to cyberattacks. Critical vulnerabilities such as SQL Injection, Directory Listing and broken authentication etc have been identified in subject website and mobile application. Exploitation of these vulnerabilities may result in compromise of webserver, remote command & control and partial authentication of users. It is also recommended that M-Tag application be thoroughly screened by 3rd party from Cyber Security aspect before its official launching. Moreover, an advisory is attached at Annexure A for compliance.

2. Disseminate the same message in your organizations, all attached / affiliated departments and ensure Cyber Security aspect of web / mobile applications that contain personally identifiable information (PII) or citizen's data. The PII or citizens data must be protected by ensuring secure software development practices, hosting services and security testing of web / mobile applications prior to their official launch.


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

To:-

Chairman (NHA),
National Highways Authority (NHA),
Islamabad.

All Secretaries of Ministries / Divisions of Federal Government and Chief Secretaries
of 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

Copy (C) No. 258
10-1-22

Cyber Security Advisory -- Vulnerable NHA website and Motorway Mobile Application (Advisory No. 92)

1. The identified vulnerabilities, their impact and recommended mitigation measures are as under :-

Ser	Vulnerability	Description	Mitigation
a.	SQL Injection (mis.nha.gov.pk) RAMD, LBMIS, PMIS (Appendix I)	An attacker may execute arbitrary statements on the vulnerable system. This may compromise integrity of Database and expose sensitive information	<ul style="list-style-type: none"> Data received from external parties must be validated such that only the value that passes the validation can be processed. By employing parameterized queries, user input is automatically quoted and the user / attacker supplied input will not cause change of the intent. This coding style helps prevent SQL injection attack. Stored procedures can reduce direct access to fractions of database, making it essential for database security. Always use character-escaping functions for user-supplied input provided by database management system (DBMS). This is done to make sure that DMBS never confuses it with SQL statement provided by developer.
b.	Weak Password RAMD, LBMIS (Appendix II)	An Attacker can access the content of web pages	Use strong passwords at all levels
c.	Directory Listing Enabled (Appendix III)	Directly listing is enabled on website that can results in increasing attack surface during exploitation and leakage of data.	Web servers should be configured to disable directory listing by default

d.	Cross Site Scripting (mis.nha.gov.pk)	Malicious users may inject JavaScript, VBScript, ActiveX, HTML or Flash into a vulnerable application to lure users to gather data from them. An attacker can steal the session cookie and take over account, impersonating the user. It is also possible to modify the content or the page presented to the user.	<ul style="list-style-type: none"> • Whenever possible prohibit HTML code in inputs • Validate Inputs. Validating the data to ensure it meets specific criteria. • Secure cookies. By setting rules for web applications defining how cookies are handled can prevent XSS and even block JavaScript from accessing cookies • Use a web application Firewall (WAF). Rules can be created on WAF to specifically address XSS by blocking abnormal server requests
e.	Insecure Communication (http://mis.nha.gov.pk) (http://nha.gov.pk)	Website communicates over insecure HTTP protocol	Incorporate secure certificate (https)
Motorway M-Tag Mobile Application (onenetwork.pk)			
f.	M-Tag Onenetwork Mobile Application; Broken Authentication Flaw (Appendix IV)	<ul style="list-style-type: none"> • An attacker can utilize Onenetwork server to send customized SMS instead of OTP to anyone with knowledge of victim's phone number. • Authentication tokens can be reused for any person and tokens are generated prior to complete user authentication. 	Two factor authentication must be ensured by sending an OTP to registered phone number only to avoid illegitimate / unauthorized access to potentially sensitive data.

Cyber Security Best Practices for Website and Mobile Application

- Upgrade OS and Webserver to latest version.**
- Website admin panel should only be accessible via white-listed IPs.**
- Vulnerability Assessment and penetration testing of application be carried out to identify potential threats on routine basis.**

- d. Complete website be deployed on inland servers including database and web infrastructure.
- e. HTTPS protocol be used for communication between client and web server.
- f. Application and database be installed on different machines with proper security hardening.
- g. Sensitive data be stored in encrypted form with no direct public access.
- h. Proper security hardening of endpoints and servers be performed and no unnecessary ports and applications be used.
- i. Updated Antivirus tools / Firewalls be used on both endpoints and servers to safeguard from potential threats.
- j. Enforce a strong password usage policy.
- k. Remote management services like RDP and SSH must be disabled in production environment.
- l. Deploy web application firewalls for protection against web attacks.
- m. Employ secure coding practices such as parameterized queries, proper input sanitization and validation to remove malicious scripts.
- n. Keep system and network devices up-to-date.
- o. For attacker's reconnaissance, Log retention policy must be devised for at least 3x months on separate device.
- p. In case of mobile applications, two factor authentication must be ensured by sending an OTP to registered phone number only to avoid illegitimate / unauthorized access to potentially sensitive data.
- q. The mobile application must communicate with secure services over https to avoid MITM attacks. Android SSL pinning must be implemented as an additional security measure at application level.
- r. Enable Android ProGuard for optimization and obfuscation of Android to thwart reverse engineering attempt.
- s. Vulnerability of mobile application must be carried out before public launch.
- t. Adhere to Mobile Application Security Best Practices available at the link <https://developer.android.com/topic/security/best-practices>.

3. **Reporting of Cyber Security Issues / Queries.** For reporting malware or any other query or issues regarding Cyber Security, details may please be forwarded to the following email address: -

asntisb2@cabinet.gov.pk

Welcome to RAMD



National Highway Authority

Form fields for user login, including a password field with a blacked-out area.

Handwritten text: 2012-01-03 03:45

- 10. Home
- 11. Login
- 12. Register

- http://www.nha.gov.ph/links/external.htm
- http://www.nha.gov.ph/links/external.htm
- http://www.nha.gov.ph/links/external.htm

Appendix II

```

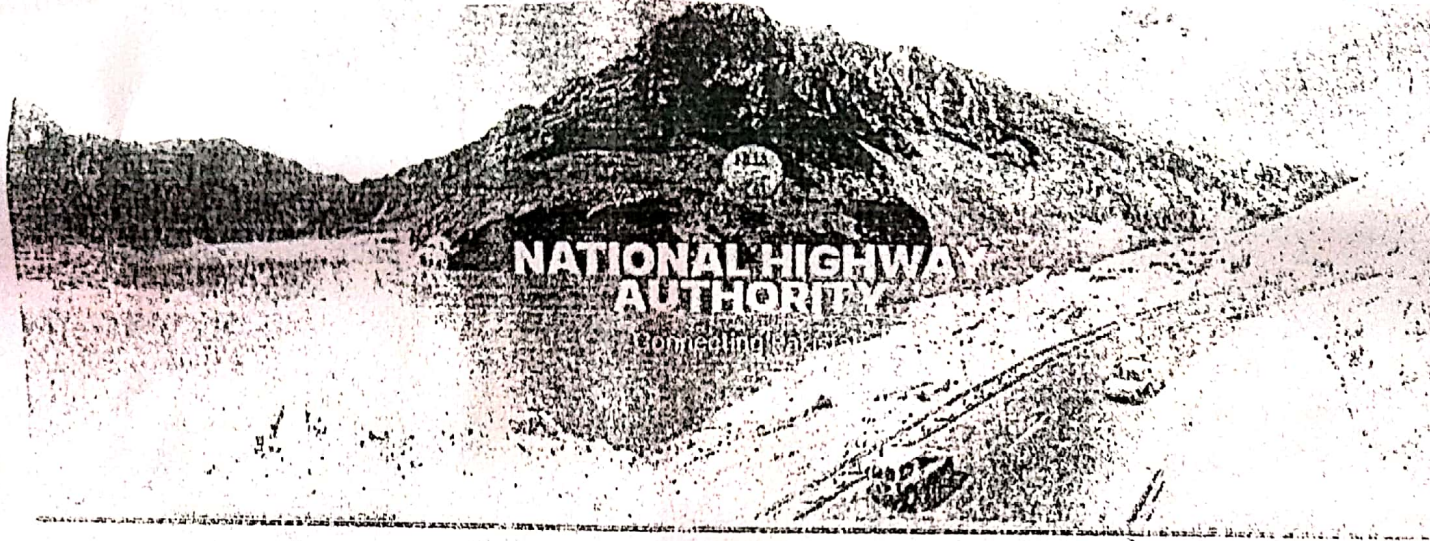
root /bin/curl/1.11.1
Content-Length: 80
Content-Type: application/x-www-form-urlencoded
Referer: http://nha.nha.gov.ph:81/
Host: nha.nha.gov.ph:81
Connection: keep-alive
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21
Accept: */*

```


22

To play video, you may need to install the required video player.

150



Appendix IV

← 44731

www.nhai.org

Enjoy it ~~5700~~ sahre
 to enjoy.
 SWZsK ih/RU

100%