NO.SO(GA)SE&LD/CERT/2026

GOVERNMENT OF SINDH
SCHOOL EDUCATION & LITERACY DEPARTMENT

Karachi, dated the 23rd April, 2026

To,

1. The Chairman, Sindh Text Book Board (STBB), Jamshoro.
2. The Director General, Planning Development & Research (PD&R).
3. The Director General, Directorate of Inspection / Reg. of Private Institutions in Sindh.
4. The Director General, Provincial Institution of Teachers Education (PITE), Nawabshah.
5. The Executive Director, Sindh Teachers Education Development Authority (STEDA).
6. The Director, Sindh Education Policy Commission (SEPC).
7. The Director, Directorate of Curriculum, Assessment & Research @ Jamshoro.
8. The Director, Directorate of Literacy & Non-formal (SE&LD).
9. The Director School Education (Primary / ES&HS) All in Sindh.
10. The Chief Engineers (Education Works), Hyderabad/Sukkur/Karachi.
11. The Chief Program Manager, Reform Support Unit (RSU).
12. The Director General, Directorate of Monitoring & Evaluation.
13. The Additional Director, Directorate of Teachers Training Institution Sindh, Hyderabad.
14. The Project Director, English Medium Project.
15. The Director, Human Resources & Training (HR&T).
16. The Senior Director, Public Private Partnership (PPP Node).
17. The Director, Inspection & registration of Government Institutions.
18. The District Education Officers (all) in Sindh.

Subject:- **CYBER SECURITY ADVISORY – CYBER SECURITY ADVISORY ON CHROME DESKTOP VULNERABILITIES AFFECTING GOVERNMENT SYSTEMS AND WINRAR PATH TRAVERSAL VULNERABILITY.**

I am directed to forward herewith the copies of letters No.DG-II/CERT/4/124/2023 dated 14.04.2026 alongwith its enclosures received from Science & Information Technology Department, Government of Sindh on the subject noted above.

It is requested to please go through the contents of the letters and take immediate necessary action for compliance of the recommended security measures under intimation to this department.

(IQBAL JUNEJO)
SECTION OFFICER (GA)
For Secretary to Govt. of Sindh

A Copy for information is forwarded to:-

1. The Special Secretary (all), School Education & Literacy Department.
2. The Additional Secretary (all), School Education & Literacy Department.
3. The Deputy Secretary (all), School Education & Literacy Department.
4. The Section Officer (all), School Education & Literacy Department.
5. PS to Secretary, School Education & Literacy Department.
6. The Office Order File.

NO.DG-II/ CERT/4/124/2023
GOVERNMENT OF SINDH
SCIENCE & INFORMATION TECHNOLOGY
DEPARTMENT-021-99213409
Karachi, Dated: 14th April, 2026

To

1. The Chairman, Planning & Development Board Sindh, Karachi
2. The Chairman, Enquires, Anti-Corruption, Establishment Sindh, Karachi.
3. The Chairman/Chairperson, CMIT Sindh, Karachi
4. The Chairman Sindh HEC Karachi.
5. The Senior Member Board of Revenue (BOR)Sindh, Karachi.
6. The Additional Chief Secretary, Govt of Sindh_____.
7. The Principal Secretary to Governor Sindh, Governor Secretariat, Karachi.
8. The Principal Secretary to Chief Minister Sindh, Chief Minister Secretariat, Karachi.
9. The Administrative Secretary, Government of Sindh (All). School Education & Literacy Deptt.
10. The Provincial Ombudsman, Sindh.
11. The Inspector General of Police Sindh, Karachi
12. The Divisional Commissioner (All) in Sindh_____.

SUBJECT: CYBERSECURITY ADVISORY – CYBERSECURITY ADVISORY ON CHROME DESKTOP VULNERABILITIES AFFECTING GOVERNMENT SYSTEMS

In view of multiple high-severity vulnerabilities recently identified in Google Chrome desktop versions (Windows, macOS, Linux), the attached advisory titled "NCA-28.040326-National CERT Advisory - Chrome Desktop Vulnerabilities" (Annexure) has been issued by the National Cyber Emergency Response Team (National CERT).

2. This advisory outlines the technical details, associated risks, and operational impacts of these vulnerabilities affecting Chrome versions prior to 141.0.7390.65/66 for Windows and macOS, 41.0.7390.65 for Linux. The identified vulnerabilities tracked as CVE-2025-11458, CVE-2025-0, and CVE-2025-11211, include memory corruption flaws such as heap buffer overflow and -after-free conditions, which may allow remote attackers to execute malicious code, cause denial service (DoS), or disclose sensitive information by luring users to specially crafted web pages.

3. Given the widespread use of Google Chrome across government ministries, departments, and critical infrastructure entities, these vulnerabilities pose a significant cybersecurity risk to desktop environments. Successful exploitation could lead to remote code execution, data compromise, system instability, or service disruption. Immediate patching of affected systerns and proactive monitoring through Endpoint Detection and Response (EDR) tools are strongly recommended to mitigate risk.

4. It is requested that the attached Advisory be disseminated to all relevant departments, agencies, and organizations under your administrative control for immediate compliance and necessary action, including verification that all Chrome installations are updated to the latest stable version.

Annexure: NCA-28.040326-National CERT Advisory - Chrome Desktop Vulnerabilities

"Disclaimer: This document contains confidential information and is not to be disclosed to the media or any public information platform."

15/4/26

(MUHAMMAD AKBAR KHAN)
SECTION OFFICER(TECH)

A copy is forwarded for information and necessary action to: -

1. Chief Executive Officer Sindh IT Company (SITC), Karachi.
2. Director General (nCERT). L Block, Pak Secretariat, Islamabad
3. PS to Chief Secretary, Sindh.
4. Staff Officer to Special Assistant to Chief Minister Sindh, S&IT Department, Govt. of Sindh, Karachi.
5. PS to Secretary I&C, SGA&CD, Govt. of Sindh, Karachi.
6. Staff Officer to Secretary S&IT Department, Govt. of Sindh, Karachi.

8203 15/4/26

20/4/26

SO(GA)

SECTION OFFICER(TECH)

Annexure

NCA-28.040326 – National CERT Advisory – Chrome Desktop Vulnerabilities

1. Introduction

Multiple high-severity vulnerabilities in Google Chrome for desktop (Windows, macOS, Linux) have been reported, affecting Chrome versions prior to 141.0.7390.65/66 for Windows, Mac and 141.0.7390.65 for Linux. Google released a stable update (Chrome 141.0.7390.65/66 for Windows/Mac, 141.0.7390.65 for Linux) to address these vulnerabilities.

2. Threat Indicators (IoC's)

a. **Vulnerabilities Identified**
Google described three highlighted issues as under: -

1) **CVE-2025-11458.** A heap buffer overflow11 in the Sync22 component, enabling an attacker to overwrite memory with harmful data, potentially forcing Chrome to execute malicious code.
2) **CVE-2025-11460.** A use-after-free33 error, causing an attacker to use memory object after it has already been deleted, allowing them to insert malicious data, hijack program flow, or crash the Chrome.
3) **CVE-2025-11211.** Vuln in WebCodecs44 can be exploited, leading Chrome to leak parts of memory, exposing sensitive info or causing minor instability; less severe than the other two.

b. Attack Vector

A remote attacker could exploit these flaws by enticing a user to visit a specially crafted web page, potentially triggering memory corruption. Exploit scenarios can lead to malicious code exec, denial of svc (crash), or info disclosure.

CamScanner

3. Risk and Impact

High Severity vulnerability could cause remote code execution, data theft, and Denial of Svc (DoS) on affected desktops.

4. Recommended CVSS Scores (for internal prioritization)

CVE ID	Vulnerability Type	Impact	CVSS v3.1 (Estimated)
CVE-2025-11458	Heap Buffer Overflow	RCE / Crash	8.8 (High)
CVE-2025-11460	Use-After-Free	RCE	9.1 (Critical)
CVE-2025-11211	Memory Corruption	Info Disclosure / RCE	8.3 (High)

5. Action Required

a. **Update Chrome.** Install latest stable update (Chrome 141.0.7390.65/.66 for Windows/Mac, 141.0.7390.65 for Linux). Verify the update via Menu → Help → About Google Chrome. The browser will auto-update or prompt to relaunch.

b. **Limit Exposure.** Block or restrict access to untrusted websites, avoid opening links from unknown senders and discourage use of browser plugins/ extensions that process remote content. Monitor endpoint detection/response (EDR) for unusual process activity.

CamScanner

NO.DG-II/ CERT/4/124/2023
GOVERNMENT OF SINDH
SCIENCE & INFORMATION TECHNOLOGY
DEPARTMENT-021-99213409
Karachi, Dated: 14th April, 2026

To

1. The Chairman, Planning & Development Board Sindh, Karachi
2. The Chairman, Enquires, Anti-Corruption, Establishment Sindh, Karachi.
3. The Chairman/Chairperson, CMIT Sindh, Karachi
4. The Chairman Sindh HEC Karachi.
5. The Senior Member Board of Revenue (BOR)Sindh, Karachi.
6. The Additional Chief Secretary, Govt of Sindh_____.
7. The Principal Secretary to Governor Sindh, Governor Secretariat, Karachi.
8. The Principal Secretary to Chief Minister Sindh, Chief Minister Secretariat, Karachi.
9. The Administrative Secretary, Government of Sindh (All). _____.
10. The Provincial Ombudsman, Sindh.
11. The Inspector General of Police Sindh, Karachi
12. The Divisional Commissioner (All) in Sindh_____.

SUBJECT: CYBERSECURITY ADVISORY – CYBERSECURITY ADVISORY ON WINRAR PATH TRAVERSAL VULNERABILITY

In view of a high-severity path traversal vulnerability recently identified in WinRAR for Windows, the attached Advisory titled "NCA-29.040326 National CERT Advisory WinRAR Path Traversal Vulnerability (Annexure) has been issued by the National Cyber Emergency Response Team (National CERT).

2. The advisory outlines the technical detalls, associated risks, and operational impacts of the vulnerability tracked as CVE-2025-8088, affecting WinRAR Windows versions up to and including 7.12. The identified flaw is a path traversal vulnerability that may allow remote attackers to execute arbitrary code by enticing users to download and open specially crafted malicious archive files. Successful exploitation could enable attackers to place malicious files within sensitive system directories, including Windows Startup folders. establishing persistent access without requiring elevated privileges.

3 Given the widespread use of WinRAR across government ministries, departments, and critical Infrastructure entities, this vulnerability poses a significant cybersecurity risk to desktop environments. Exploitation may result in remote code execution with the privileges of the logged-in user, persistence mechanisms through unauthorized startup entries, system compromise, and potential disruption of services. Immediate upgrading to WinRAR version 7.13 or later, along with inspection of startup applications and proactive endpoint monitoring, is strongly recommended to mitigate associated risks.

4 It is requested that the attached Advisory be disseminated to all relevant departments, agencies, and organizations under your administrative control for immediate compliance and necessary action. This includes verification that all WinRAR installations are updated to the latest secure version and that recommended preventive and monitoring measures are implemented.

Annexure: NCA-29.040326-National CERT Advisory-WinRAR Path Traversal Vulnerability.

"Disclaimer: This document contains the media or any public information platform" and is not to be disclosed to media or any public information platform.

(MUHAMMAD AKBAR KHAN)
SECTION OFFICER(TECH)

A copy is forwarded for information and necessary action to: -

1. Chief Executive Officer Sindh IT Company (SITC), Karachi.
2. Director General (nCERT). L Block, Pak Secretariat, Islamabad
3. PS to Chief Secretary, Sindh.
4. Staff Officer to Special Assistant to Chief Minister Sindh, S&IT Department, Govt of Sindh, Karachi.
5. PS to Secretary I&C, SGA&CD, Govt. of Sindh, Karachi.
6. Staff Officer to Secretary S&IT Department, Govt. of Sindh, Karachi.

SECTION OFFICER(TECH)

Annexure

NCA-29.040326 – National CERT Advisory – Winrar Patch Traversal Vulnerability

1. Introduction

WinRAR is a widely used file archiving utility across various public and private organizations. Recently, a high-severity path-traversal vulnerability, **CVE-2025-8088**, has been discovered. The flaw resides specifically within the UnRAR.dll component in WinRAR Windows versions up to and including **7.12**. This vulnerability allows attackers to execute arbitrary code by crafting malicious archive files.

2. Threat Details

a. Attack Vector

A remote attacker can exploit this flaw by enticing a user to download and open a specially crafted malicious archive file. Upon opening or extracting the file, the vulnerability in the UnRAR.dll component is triggered. This allows the attacker to execute malicious code by manipulating memory variables stored within the operating system.

b. Risk & Impact

1) Arbitrary Code Execution: Attackers can run malicious commands with the same privileges as the logged-in user.
2) Startup Manipulation: The path-traversal nature allows attackers to place malicious files directly into Windows Startup directories.
3) Persistence: Attackers can establish persistent access to the compromised system without requiring administrative elevation.

Priority	Action	Timeline
MANDATORY	Update to WinRAR 7.13 Final	Immediate
HIGH	Inspect Startup folder/services	Within 24 hours
HIGH	Scan all .rar archives with Antivirus	Ongoing
REQUIRED	Block RAR downloads from untrusted sources	Continuous

CamScanner

National Cyber Emergency Response Team
Government of Pakistan

3. Remediation & Action Requested

a. Immediate Software Update

- Upgrade to WinRAR 7.13 Final (released July 30, 2025) or later immediately. This version contains the official patch for the UnRAR.dll component.

b. System Inspection & Cleaning

- Startup Folder Review: Inspect the Windows Startup folder for any unknown executables or shortcuts.
- Disable Suspicious Apps:
  1. Press the Windows Key and type Startup Apps in the search bar.
  2. Review the list of applications and services set to run at login.
  3. Disable any unknown or suspicious applications.

c. General Security Hygiene

- Anti-Virus Update: Ensure your anti-virus definitions are up to date to detect known exploit patterns associated with this CVE.
- Source Verification: Avoid clicking links or opening archive files (RAR/ZIP) received from unknown or untrusted sources.
- Safe Browsing: Only download software and files from trusted, official websites.

4. INCIDENT REPORTING

Any suspected exploitation of this vulnerability or discovery of suspicious Startup entries should be reported immediately to National CERT Pakistan:

- Incident Reporting Portal: https://pkcert.gov.pk/report-incident/
- Email: cert@pkcert.gov.pk
- UAN: +92 519203412

National Cyber Emergency Response Team (NCERT)
Government of Pakistan
Pak Secretariat, L Block, Islamabad, Pakistan
+92-51-9203422 | info@pkcert.gov.pk | www.pkcert.gov.pk

CamScanner

5. CALL TO ACTION – KEY IMPERATIVES

a. Update all Windows installations of WinRAR to version 7.13 Final immediately.
b. Verify the integrity of Windows Startup folders across all workstations.
c. Educate staff on the risks of opening unsolicited archive files.

WARNING: Failure to patch CVE-2025-8088 may allow an adversary to gain a persistent foothold in your network, leading to data exfiltration and further lateral movement.

CamScanner

NO.DG-II/ CERT/4/124/2023
GOVERNMENT OF SINDH
SCIENCE & INFORMATION TECHNOLOGY
DEPARTMENT-021-99213409
Karachi, Dated: 14th April, 2026

To

1. The Chairman, Planning & Development Board Sindh, Karachi
2. The Chairman, Enquires, Anti-Corruption, Establishment Sindh, Karachi.
3. The Chairman/Chairperson, CMIT Sindh, Karachi
4. The Chairman Sindh HEC Karachi.
5. The Senior Member Board of Revenue (BOR)Sindh, Karachi.
6. The Additional Chief Secretary, Govt of Sindh_____.
7. The Principal Secretary to Governor Sindh, Governor Secretariat, Karachi.
8. The Principal Secretary to Chief Minister Sindh, Chief Minister Secretariat, Karachi.
9. The Administrative Secretary, Government of Sindh (All). _____.
10. The Provincial Ombudsman, Sindh.
11. The Inspector General of Police Sindh, Karachi
12. The Divisional Commissioner (All) in Sindh_____.

SUBJECT: CYBERSECURITY ADVISORY ON APT SIDEWINDER PHISHING CAMPAIGN TARGETING GOVERNMENT ORGANIZATIONS

In view of a recently observed targeted phishing campaign attributed to the Indian-ongin Advanced Persistent Threat (APT) group SideWinder (also tracked as Rattlesnake, Hardcore Nationalist (HN2), and T-APT-04) the attached advisory titled ""NCA-30.070326-National CERT Advisory - APT SideWinder - Phishing Attack **Government Organizations" (Annexure**) has been issued by the National Cyber Emergency Response Team (National CERT)

2. The advisory outlines the nature, risks, and operational impacts of this ongoing phishing campaign, which specifically targets employees of Pakistani public sector organizations through impersonated domains and malicious files. The threat actor has registered multiple deceptive domains masquerading as legitimate government entities to harvest credentials and facilitate follow-on intrusions.

3. Given the campaign's deliberate targeting of key government organizations including the Cabinet Division, Ministry of Defence, Ministry of Finance, Ministry of Commerce, NEPRA, and National CERT, this operation poses a serious threat to Pakistan's public sector, defense, and critical infrastructure entities. Immediate blocking and flagging of the dentified Indicators of Compromise (loCs) across Email servers, Firewalls, Endpoint Detection and Response (EDR) tools, and Security Information and Event Management (SIEM) systems is strongly recommended to mitigate risk.

4 Recipient organizations are requested to treat this matter with utmost urgency. The attached Advisory (Annexure) contains detailed technical insights into the threat actor's tactics, techniques, and procedures (TTPs) identified malicious domains/URLs, and recommended preventive and defensive measures for users and system administrators.

5. It is requested that the attached Advisory be disseminated to all relevant departments, agencies, and organizations under your administrative control for immediate compliance and necessary action.

Annexure: NCA-30.070326 - National CERT Advisory - APT SideWinder - Phishing Attack on Government Organizations

"Disclaimer: This document contains confidential information and is not to be disclosed to the media or any public information platform"

(MUHAMMAD AKBAR KHAN)
SECTION OFFICER(TECHNICAL)

A copy is forwarded for information and necessary action to: -

1. Chief Executive Officer Sindh IT Company (SITC), Karachi.
2. Director General (nCERT). L Block, Pak Secretariat, Islamabad
3. PS to Chief Secretary, Sindh.
4. Staff Officer to Special Assistant to Chief Minister Sindh, S&IT Department, Govt. of Sindh, Karachi.
5. PS to Secretary I&C, SGA&CD, Govt. of Sindh, Karachi.
6. Staff Officer to Secretary S&IT Department, Govt. of Sindh, Karachi.

SECTION OFFICER(TECHNICAL)

Annexure

NCA-30.070326 – National CERT Advisory – APT Sidewinder - Phishing Attack on Government Organizations

1. Introduction

A sophisticated phishing campaign has been launched by the Indian-origin Advanced Persistent Threat (APT) group known as "SideWinder" (also tracked as Rattlesnake, Hardcore Nationalist (HN2), and T-APT-04). Active since 2012, this group is historically engaged in cyber espionage against government and military institutions in South Asia. The current campaign aggressively targets employees of Pakistani public sector organizations through the use of impersonated domains and malicious files. The Threat Actor (TA) has registered several fake domains to lure victims, necessitating the immediate blocking and flagging of the identified Indicators of Compromise (IoCs) on all organizational Email servers, Firewalls, Endpoint security solutions, and Security Information and Event Management (SIEM) systems.

2. Threat Indicators (IoCs)

The following malicious domains and files have been identified as part of this campaign and require immediate action:

Ser	Malicious Domains / URLs	Impersonated Organizations	Malicious File / Link
a.	cabinet-gov-pk[.]fetchdrive[.]org	Cabinet Div	-
b.	buildtheations[.]info/Build_Nation	Ministry of Defence (MOD)	https://nepra.org
c.	(1) finance-gov-tpk[.]fetchdrive[.]org/ (2) finance-gov-tpk[.]grabfiles[.]net/	Ministry of Finance	-
d.	nepra-org-pk[.]grabfiles[.]net/	NEPRA	-
e.	Commerce-gov-pk[.]fetchdrive[.]org	Ministry of Commerce	-
f.	buildtheations[.]info/PKCERT/pkcert.html	National CERT	https://nepra.org

CamScanner

National Cyber Emergency Response Team
Government of Pakistan
PKCERT

3. Action Requested

All recipient organizations are requested to treat this as an urgent alert.

a. **Directorate General ISI Only:** The domains listed above are requested to be flagged at the highest priority.
b. **All Setups:** The domains and URLs in the table above must be immediately blocked on email servers, Firewalls, Endpoint Detection and Response (EDR) tools, and SIEM solutions to prevent any interaction from users within the network.

4. Deploy Detection Rules

Endpoint Detection & Response (EDR)

a. Detect Microsoft Office applications spawning command interpreters or PowerShell processes
b. Monitor abnormal child processes initiated by email attachments
c. Alert on credential dumping or suspicious privilege escalation behavior

5. Execute Immediate Technical Mitigation Actions (24-Hour Response)

1. Block all identified malicious domains, URLs, and IP addresses at gateway and DNS levels
2. Reset credentials for users interacting with suspected phishing infrastructure
3. Review previous 14 days of email gateway, proxy, and EDR telemetry logs
4. Enforce Multi-Factor Authentication (MFA) across email, VPN, and privileged systems
5. Validate and enforce SPF, DKIM, and DMARC configurations
6. Disable or isolate compromised user accounts immediately
7. Verify integrity of backups and ensure offline backup availability

6. Modus Operandi - Phishing Attacks

a. In this particular campaign TA attempts to steal victim's credentials email for launching of further phishing attacks.
b. Cyber Threat Actor (TA) sends deceptive emails or links/files/media that appear to originate from trusted sources (Govt offices, banks, online services etc).
c. Emails/ links contain official messages/ orders or some appealing content such as security alert instructions, account suspension warnings or password reset requests, urging the receiver for immediate action.

National Cyber Emergency Response Team (NCERT)
Government of Pakistan
Pak Secretariat, L Block, Islamabad, Pakistan
+92-51-9203422 | info@pkcert.gov.pk | www.pkcert.gov.pk

CamScanner

7. Potential Consequences.

Following are possible consequences if attack remained successful:

a. Credentials Compromise.

b. System compromise for expanding malicious ingress.

c. Installation of malware.

8. Suggested Measures - Users & Administrators

a. **Communication Vigilance:**

1. All users and administrators are advised to remain vigilant regarding phishing emails. Moreover, all organizations' administrators are advised to change all user passwords for their mail server.

2. Verify identities through independent channels if any email or msg claims affiliation with relevant organizations.

b. **Device Security:** Update Email, other social media applications and device operating system regularly to **patch vulnerabilities**.

c. **Digital Hygiene:**

(1) Do not click on **unknown links & URLs** received through emails, social & communication media.

(2) Strong password policy & multifactor authentication be implemented for all users.

(3) Email spam filter on mail server settings be set to max security level.

(4) AV & URL/ Link scanners be integrated with email server for scanning of email attachments before receipt by users.

(5) Personal mobile phones must not be connected to official PCs/ Laptops.

d. **Use Reputable Security Software:** Keep your AV and anti-malware software up-to-date and actively scan your system for threats.

CamScanner

13

NO.DG-II/ CERT/4/124/2023
GOVERNMENT OF SINDH
SCIENCE & INFORMATION TECHNOLOGY
DEPARTMENT-021-99213409
Karachi, Dated: 14th April, 2026

To

1. The Chairman, Planning & Development Board Sindh, Karachi
2. The Chairman, Enquires, Anti-Corruption, Establishment Sindh, Karachi.
3. The Chairman/Chairperson, CMIT Sindh, Karachi
4. The Chairman Sindh HEC Karachi.
5. The Senior Member Board of Revenue (BOR)Sindh, Karachi.
6. The Additional Chief Secretary, Govt of Sindh_____.
7. The Principal Secretary to Governor Sindh, Governor Secretariat, Karachi.
8. The Principal Secretary to Chief Minister Sindh, Chief Minister Secretariat, Karachi.
9. The Administrative Secretary, Government of Sindh (All). _____.
10. The Provincial Ombudsman, Sindh.
11. The Inspector General of Police Sindh, Karachi
12. The Divisional Commissioner (All) in Sindh_____.

SUBJECT: CYBERSECURITY ADVISORY IMPLEMENTATION OF READ ONLY MODE FOR OFFICIAL WEB PORTALS-IMMEDIATE ACTION REQUIRED

National Cyber Response Team (nCERT) 's advisory attached to ensure implementation /compliance, please

14/04/2026
(MUHAMMAD AKBAR KHAN)
SECTION OFFICER (TECHNICAL)

A copy is forwarded for information and necessary action to: -

1. Chief Executive Officer Sindh IT Company (SITC), Karachi.
2. Director General (nCERT). L Block, Pak Secretariat, Islamabad
3. PS to Chief Secretary, Sindh.
4. Staff Officer to Special Assistant to Chief Minister Sindh, S&IT Department, Govt. of Sindh, Karachi.
5. PS to Secretary I&C, SGA&CD, Govt. of Sindh, Karachi.
6. Staff Officer to Secretary S&IT Department, Govt. of Sindh, Karachi.

SECTION OFFICER (TECHNICAL)

NCA-26.280226 – NCERT Advisory: Mandatory Read-Only Mode for Government & Federal Websites

1. Introduction

In response to heightened regional tensions and the surge in hacktivist activity, National CERT directs all government and federal entities to transition their web portals to a "Read-Only" state. This measure is designed to preserve the integrity of official information and shield the national digital infrastructure from targeted disruption and disinformation campaigns.

2. Impact and Risks

Unrestricted web functionality during a crisis poses several high-severity risks:

a. **Unauthorized Defacement**: Attackers modifying homepages to display adversary propaganda or fake news.

b. **Database Injection**: Exploitation of entry fields to execute SQL injections or exfiltrate sensitive citizen data.

c. **Malicious File Uploads**: Using "Upload" features to install web shells for persistent remote access to government servers.

d. **Resource Exhaustion**: Abuse of complex backend queries to launch localized Denial of Service (DoS) attacks.

3. Threat Details

3.1 Attack Vectors

a. **Interactive Element Exploitation**: Targeting search bars, contact forms, and login portals to inject malicious code.
b. **CMS Vulnerabilities**: Exploiting unpatched plugins or themes in Content Management Systems.
c. **Unauthorized Data Modification**: Attempting to overwrite or delete server-side data through public interfaces.
d. **Credential Abuse**: Using brute-forced administrative credentials to modify web content.

CamScanner

National Cyber Emergency Response Team
Government of Pakistan
PKCERT

3.2 Threat Actors

a. **State-Sponsored APT Groups**: Sophisticated actors focusing on long-term infiltration and psychological operations.
b. **Hacktivists**: Ideologically motivated groups seeking to deface government portals for visibility.

3.3 Affected Systems

a. **Federal and Provincial Portals**: All official websites accessible to the general public.

b. **Government Databases**: Backend systems linked to interactive web forms.

c. **Citizen Services Portals**: Platforms providing interactive online services.

4. Recommendations & Mitigation Measures

4.1 Immediate Technical Actions:

a. **Restrict Modification Requests**: Configure web servers (Nginx, Apache, IIS) or Web Application Firewalls (WAF) to only allow data retrieval actions.

b. **Disable Forms and Logins**: Deactivate all interactive elements, including contact forms, search bars, and administrative login portals to eliminate entry points for attackers.

c. **Database Hardening**: Revoke "Write" and "Update" permissions for the web application's database user to ensure the backend remains untampered.

4.2 Infrastructure Hardening:

a. **Content Delivery Network (CDN)**: Leverage CDNs to serve cached versions of the website, reducing direct interaction with the origin server and mitigating DDoS risks.

b. **File Integrity Monitoring (FIM)**: Deploy tools to monitor and alert on any unauthorized change to the website's source code or file structure.

c. **IP Access Control**: Restrict access to the website backend (SSH, FTP, CMS Dashboard) to authorized internal IP addresses only.

4.3 Disaster Recovery & Continuity

a. **Static Snapshots**: Create a static HTML version of the portal that can be deployed instantly if the dynamic environment is compromised.

National Cyber Emergency Response Team (NCERT)
Government of Pakistan
Pak Secretariat, L Block, Islamabad, Pakistan
+92-51-9203422 | info@pkcert.gov.pk | www.pkcert.gov.pk

CamScanner

b. **Offline Backups**: Maintain recent, air-gapped backups of the website and database for rapid restoration.

4.4 Patching & Updates Focus

Risk	Recommendation
CMS Vulnerabilities	Patch WordPress/Drupal/Joomla and all plugins to the latest version.
Unauthorized Access	Mandate MFA for all web administration and hosting accounts.
Data Integrity	Revoke write permissions for web-user database accounts immediately.
DDoS/Resource Abuse	Route traffic through a CDN to cache static content and absorb traffic spikes.

5. Call to Action

The National CERT strongly advises all government departments to immediately implement the "Read-Only" posture. IT teams must proactively monitor web logs for unauthorized modification attempts and ensure that all interactive entry points are sealed. Any incident or suspicious activity must be reported to National CERT at **cert@pkcert.gov.pk**.

CamScanner