

NCA-17.240826 – National CERT Advisory

Adobe Acrobat Chrome Extension Vulnerability Exposing WhatsApp Web Sessions

A security vulnerability has been identified in the Adobe Acrobat Chrome Extension that could allow malicious websites to access sensitive information from an active WhatsApp Web session. The vulnerability, tracked as CVE-2026-48294, affects Adobe Acrobat Chrome Extension versions 26.5.2.2 and earlier.

An attacker can exploit this vulnerability by convincing a user to visit a specially crafted or compromised website. Once triggered, the vulnerability may allow unauthorized access to information displayed in the user's WhatsApp Web session without requiring malware installation or credential theft. Adobe has released a security update to address this vulnerability.

DOCUMENT SUMMARY

Field	Details
Advisory ID	NCA-17.240826
Threat Type	Cross-Origin Information Disclosure, Unauthorized Access to Active Web Sessions
Severity	Medium–High (Requires User to Visit a Malicious Website — Not Independently Rated in Source Advisory)
Attack Vector	Remote exploitation via a specially crafted or compromised website visited by the victim, leveraging the Adobe Acrobat Chrome Extension to access an active WhatsApp Web session
Authentication Required	None exploits an already-authenticated WhatsApp Web session present in the browser
User Interaction	Required, victim must visit a malicious or compromised website
CVSS Score	Not publicly disclosed in source advisory
Scope & Applicability	Google Chrome users with the Adobe Acrobat Chrome Extension installed and an active WhatsApp Web session
Affected Products	Adobe Acrobat Chrome Extension: versions 26.5.2.2 and earlier
Security Advisory Source	Adobe Security Advisory (CVE-2026-48294), as referenced in the source Cybersecurity Advisory Report dated 30 July 2026

IMPACT ANALYSIS

Successful exploitation of this vulnerability may allow attackers to:

1. Access information displayed in an active WhatsApp Web session

2. View chat lists, contact names, and message previews
3. Read the contents of open conversations
4. Access profile information associated with WhatsApp Web
5. Compromise user privacy and expose sensitive communications
6. Bypass browser security protections through a malicious webpage

THREAT CHARACTERISTICS

Field	Details
Threat Category	Browser Extension Vulnerability / Cross-Origin Data Exposure
Threat Status	Vendor-acknowledged; Adobe has released a security update addressing CVE-2026-48294
Root Cause	A flaw in the Adobe Acrobat Chrome Extension that allows malicious websites to access sensitive information from an active WhatsApp Web session
Attack Surface	Adobe Acrobat Chrome Extension running in Google Chrome alongside an active WhatsApp Web session
Attack Complexity	Low once a victim is lured to a specially crafted or compromised website; no malware installation or credential theft required
Privileges Required	None beyond convincing the victim to visit a crafted website
Impact Scope	Unauthorized access to WhatsApp Web chat lists, contacts, message content, and profile information; bypass of browser security protections via the malicious webpage
CWE Classes	Not specified in source advisory (consistent with CWE-346 – Origin Validation Error / CWE-200 – Exposure of Sensitive Information, based on the vulnerability description)

VULNERABILITY DETAILS

- CVE-2026-48294: Vulnerability in the Adobe Acrobat Chrome Extension that allows malicious websites to access sensitive information from an active WhatsApp Web session.
 - Affected Versions: Adobe Acrobat Chrome Extension 26.5.2.2 and earlier.
 - Fixed Version: Adobe has released a security update addressing this vulnerability (specific patched build number not stated in source advisory).
 - Exploitation Prerequisite: Requires the attacker to convince a user to visit a specially crafted or compromised website; does not require malware installation or credential theft.

INDICATORS OF EXPOSURE / TARGETING (IoEs)

Organizations should actively hunt for the following indicators within browser activity, extension inventories, and user-reported behavior:

1. Browser & Website Indicators

- Unexpected redirection after visiting a website — the browser unexpectedly navigates or refreshes after opening an unfamiliar webpage.
- Unusual browser activity — background tabs or browser windows opening without user action.
- Suspicious websites requesting interaction — untrusted websites prompting users to click buttons or open documents.

2. WhatsApp & Extension Indicators

- Unexpected access to WhatsApp Web — WhatsApp Web behaves unusually after visiting a website.
- Outdated Adobe Acrobat Chrome Extension — extension version is 26.5.2.2 or earlier.
- Unauthorized access to WhatsApp messages — chats or message content appear to have been viewed without authorization.

REMEDIATION ACTIONS

1. Immediate Defensive Controls

Action Category	Recommended Actions
Patch Management	Update the Adobe Acrobat Chrome Extension to the latest available version.
Link Hygiene	Avoid opening links received from unknown or untrusted sources.
Browsing Caution	Be cautious when visiting unfamiliar websites, especially those received through emails or messages.
Browser Hardening	Keep Google Chrome and all browser extensions updated with the latest security patches.
Extension Minimization	Use only trusted browser extensions that are necessary for work.
Reporting	Report any suspicious browser behavior or suspected compromise to IT support or the cybersecurity team immediately.
Extension Review	Regularly review installed browser extensions and remove those that are no longer required.

2. Enhanced Monitoring & Detection

- Monitor for unexpected browser redirection or page refresh events after visiting unfamiliar websites.
- Track background tabs or windows opening without user action.
- Monitor WhatsApp Web sessions for unusual or unauthorized behavior.
- Track extension versions across managed endpoints to identify outdated Adobe Acrobat Chrome Extension installs.

3. Incident Response Requirements

Organizations should:

- Investigate reports of unusual WhatsApp Web or browser activity promptly.
- Review the affected endpoint's browser session, tabs, and installed extension list.
- Confirm whether the Adobe Acrobat Chrome Extension has been updated to a patched version.
- Advise affected users to review WhatsApp Web linked devices and log out of unrecognized sessions.
- Preserve browser and network logs for cases of suspected compromise.

ACTION SUMMARY & RESPONSE PRIORITIES

Action Type	Specific Steps
Patch Deployment	Update the Adobe Acrobat Chrome Extension to the latest available version.
User Awareness	Reinforce caution with unfamiliar links and websites, especially from emails or messages.
Extension Hardening	Review and minimize installed browser extensions to only those necessary for work.
Threat Hunting	Monitor for the browser and WhatsApp Web indicators listed above.
Incident Escalation	Report confirmed compromises to National CERT.

MONITORING & DETECTION REQUIREMENTS

1. Monitor for unexpected browser redirection or page refresh after visiting unfamiliar websites.
2. Track background tabs or windows opening without user action.
3. Monitor WhatsApp Web sessions for unusual or unauthorized activity.
4. Detect outdated Adobe Acrobat Chrome Extension installations (26.5.2.2 or earlier).
5. Track suspicious websites prompting users to click buttons or open documents.
6. Monitor for unauthorized viewing of WhatsApp chats or message content.
7. Audit installed browser extensions across managed endpoints.
8. Correlate browser activity logs with reported user incidents.
9. Track patch and update compliance for Chrome and browser extensions.
10. Monitor for repeated visits to known malicious or compromised domains.

INCIDENT REPORTING

All suspected compromises, exploitation attempts, or anomalous activity related to this vulnerability must be immediately reported to National CERT Pakistan:

- Incident Reporting Portal: <https://pkcert.gov.pk/report-incident/>
- Email: cert@pkcert.gov.pk

- UAN: +92 519203412

CALL TO ACTION – KEY IMPERATIVES

#	Requirement
1	Update the Adobe Acrobat Chrome Extension to the latest available version immediately.
2	Avoid opening links received from unknown or untrusted sources.
3	Exercise caution when visiting unfamiliar websites, especially those from emails or messages.
4	Keep Google Chrome and all browser extensions updated with the latest security patches.
5	Use only trusted browser extensions that are necessary for work.
6	Regularly review installed browser extensions and remove those no longer required.
7	Report suspicious browser behavior or suspected compromise to IT support or the cybersecurity team immediately.
8	Escalate confirmed compromises or indicators of exploitation to National CERT.

