

Cyber Threat Advisory

Adobe Acrobat Chrome Extension Vulnerability

Cross-Origin Data Exposure



CATEGORY

Cross-Origin Data Exposure



SEVERITY

High - Medium



PLATFORMS

Google Chrome users with the Adobe Acrobat Chrome Extension installed and an active WhatsApp Web session

IMPACT

- **Credential Theft**
- **View chat lists, contact names, and message previews**
- **Read the contents of open conversations**
- **Access profile information associated with WhatsApp Web**
- **Compromise user privacy and expose sensitive communications**
- **Bypass browser security protections through a malicious webpage**

Description

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.

Indicator of Exposure (IoEs)

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

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.

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- Outdated Adobe Acrobat Chrome Extension — extension version is 26.5.2.2 or earlier.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

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.

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.

Cyber Threat Advisory

Secure your byte world