

Why This Advisory?

In a recent bulletin, the Indian Computer Emergency Response Team (CERT-In) classified a set of newly discovered vulnerabilities in Google Chrome for Desktop as “High Severity” under reference ID CIVN-2025-0099. This alert applies to all users of Chrome versions released prior to 136.0.7103.113/114 for Windows and Mac and 136.0.7103.113 for Linux systems.

The timing of this advisory is significant. As global browser usage continues to grow, threat actors are increasingly targeting popular platforms like Chrome to carry out focused attacks. Considering that browser sessions often have links to email, financial platforms, and enterprise applications, the impact of unpatched vulnerabilities is extensive.

Technical Overview

Recent assessments have revealed multiple high-risk vulnerabilities in older versions of Google Chrome for Desktop. These flaws stem from inadequate enforcement of internal browser policies and insufficient validation of runtime handles. Together, they create a significant risk that could allow attackers to execute malicious code remotely, potentially without any user awareness or interaction.

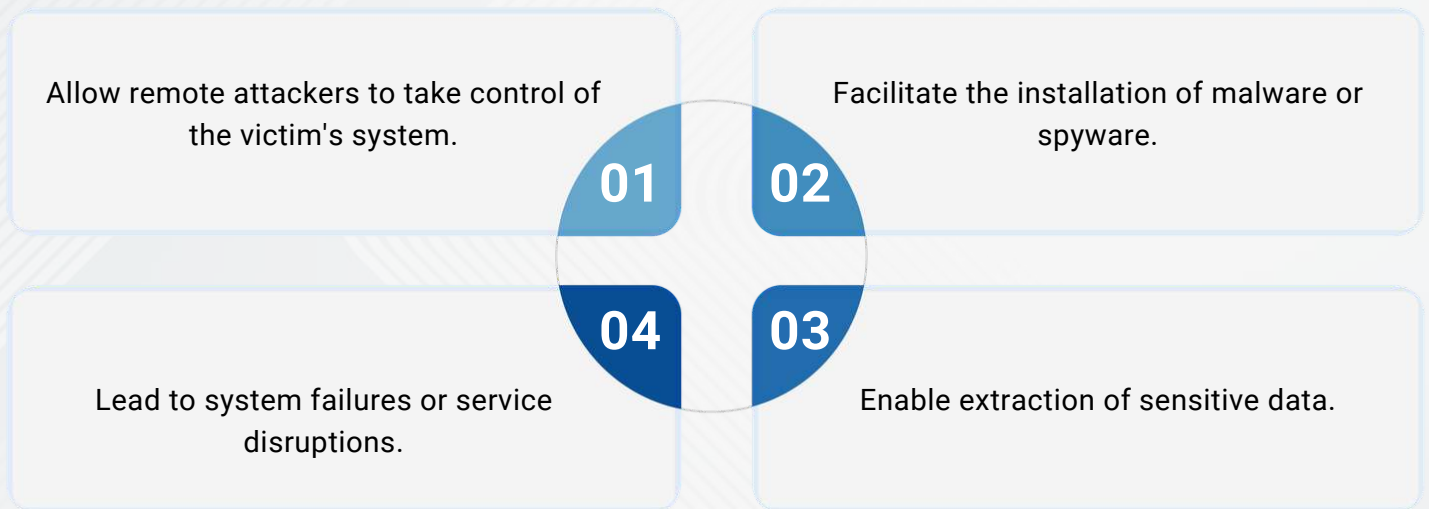
What makes this development particularly concerning is that the vulnerability—CVE-2025-4664—is already being exploited in the wild. This active exploitation significantly raises the threat landscape, especially for users who have not updated their browsers to the latest secure version. The vulnerability allows for remote code execution, giving attackers a discreet pathway to compromise user systems.

Exploitation often begins when unsuspecting users are directed to compromised or deliberately crafted websites. In other cases, malicious advertisements serve as the delivery mechanism. Once activated, these elements exploit underlying vulnerabilities, leading to immediate system compromise and possibly extended unauthorized access.



Potential Impact

If exploited, these vulnerabilities could



Immediate Action for All Users

Step 01

Update Google Chrome Immediately.

- Open Chrome, click the three dots, navigate to Help, then select About Google Chrome.
(Chrome Menu (:)) → Help → About Google Chrome)
- Make sure you're on version 136.0.7103.113/114 or higher.
- Restart your browser to finish the update.

Step 02

Disable Automatic Media Downloads

Especially for enterprise devices that have a high exposure risk

Step 03

Implement Browser Controls for Organizations

- Utilize Chrome Enterprise Admin to restrict outdated versions.
- Implement Software Restriction Policies or AppLocker to prevent vulnerable instances.