

[Security](#)

April 23, 2009 6:06 PM PDT

Google fixes severe Chrome security hole

by [Stephen Shankland](#)[Font size](#)[Print](#)[E-mail](#)[Share](#)[Yahoo! Buzz](#)

Google released a new version of its [Chrome browser](#) Thursday to fix a high-severity security problem.

The problem affects Google's mainstream stable version of Chrome and is fixed in the new version [1.0.154.59 \(download\)](#). Google has built Chrome so it updates itself automatically with no user intervention, though the software must be restarted for the new version to run.



The [security problem](#), reported April 8 by Roi Saltzman of the IBM Rational Application Security Research Group, allowed cross-site scripting attacks. Such methods can make a Web browser process unauthorized code such as JavaScript, enabling a variety of attacks, including impersonation or phishing.

Mark Larson, Google Chrome program manager, described the problem this way in a [blog posting](#) Thursday:

An error in handling URLs with a chromehtml: protocol could allow an attacker to run scripts of his choosing on any page or enumerate files on the local disk under certain conditions.

If a user has Google Chrome installed, visiting an attacker-controlled Web page in Internet Explorer could have caused Google Chrome to launch, open multiple tabs, and load scripts that run after navigating to a URL of the attacker's choice. Such an attack only

works if Chrome is not already running.



Stephen Shankland covers Google, Yahoo, search, online advertising, portals, digital photography, and related subjects. He joined CNET News in 1998 and since then also has covered servers, supercomputing, open-source software, and science. [E-mail Stephen](#), or follow him on Twitter at <http://www.twitter.com/stshank>.

Topics: [Vulnerabilities & attacks](#)

Tags: [Chrome](#), [browsers](#), [Google](#), [security](#), [XSS](#), [cross-site scripting](#)

Share: [Digg](#) [Del.icio.us](#) [Reddit](#) [Yahoo! Buzz](#) [Facebook](#)

Related

From CNET

[F-Secure says stop using Adobe Acrobat Reader](#)

[Gmail now knows who you want to e-mail](#)

[Chrome update offers tab micromanagement options](#)

From around the web

[Conficker Removal Reminders](#)

Washington Post Blogs - Faster...

[Google Chrome - Next A Google OS?](#) Lockergnome

[More related posts](#)

powered by



Sphere