

[Print](#)

Google Chrome security bests other browsers in two ways: researchers

In an in-depth analysis of browser security across many different aspects, Accuvant Labs shows that Google Chrome is beating out Internet Explorer and Mozilla Firefox. But all browsers are becoming more secure because of competition.

11/3/2011 7:49:00 AM

by Brian Jackson

Google Chrome may be a relatively new browser compared to Microsoft's Internet Explorer and Mozilla Firefox, but it's making better efforts on a couple of key security fronts, according to researchers at Accuvant Labs.

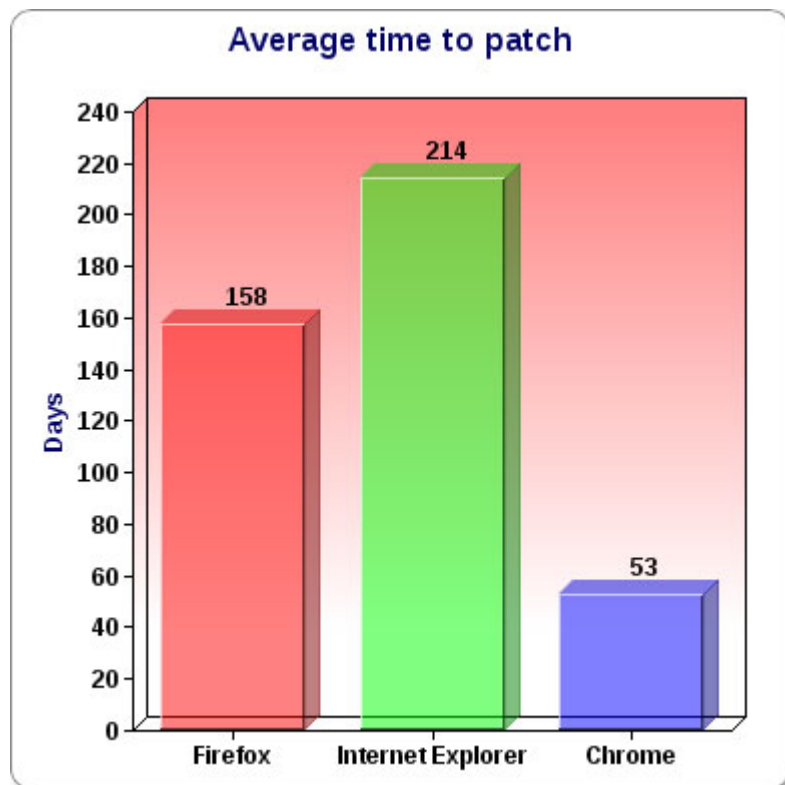


The Denver-based security solutions provider says it has been doing months of research on the latest versions of the [browsers](#), unleashing malicious payloads in a test environment and monitoring how well each one absorbed the threat. The researchers unveiled a first glimpse at their results at Toronto's Sector conference in October.

"The browser has become the most critical application we all use, and in some cases the only application we all use," says Shawn Moyer, practice manager of research consulting at [Accuvant Labs](#). "Ultimately the best browser is the most payload hostile one."

Related Story | [Dell's free browser security tool protects SMBs](#)

Accuvant researchers included the average time it took Microsoft Corp., Mozilla, and Google Inc. in their study. They found that [Internet Explorer](#) remained vulnerable for the longest average time after an exploit was discovered, at 214 days to patch. Mozilla issued its patches to Firefox in an average of 158 days, and [Chrome](#) was patched in an average of 53 days.



Number of days on average taken to patch a new exploit.

"That doesn't necessarily reflect well on the [Chrome](#) team, since their internal policy is 30 days to patch," Moyer says.

Sandboxing to security

One method browsers can be used for security is to manage tasks across various operating system processes. In Windows 7 for example, application processes are divided into security levels deemed low, medium, high, and system. Most applications run at medium level to allow for writing to directories, but browsing processes are often low-level to provide read only access.

Processes can be used to isolate, or "sandbox," certain risky applications so they don't affect other applications running on a computer. Applications also have the option to run different processes to segregate their operations.

Each browser is built with a different architecture when it comes to processes, explains Paul Mehta, senior research scientist at Accuvant. "Sandboxing and multi-process architectures are the biggest steps forward in browser security in recent years."

Internet Explorer runs a "loosely coupled" process mode, Mehta says. It allows for one medium-integrity broker process and creates low-integrity processes for materials rendered by the browser. That way browsing tabs, ActiveX controls and other plugins are sandboxed in.

Chrome has a similar approach, but creates a new out-of-process procedure for each task it runs. This limits the risk for each component of the browser, he says.

Firefox is the contrarian of the bunch, running everything on a single process. That allows for advantage such as an easier path for developers to build extensions and add-ons, but could lead to security compromises.

"If you're running your banking in one tab, and Flash in another, if one gets compromised, they could see each other," he says.

Blacklisting offers little benefit

Each browser runs its own URL blacklist service, Moyer says. But this won't defend against highly-targeted attacks, just mass malware and phishing campaigns that operate blindly. Blacklists create a list of URLs known to be used for distributing malware and will cause browsers to either prevent users from going there, or provide a warning before they do.

Internet Explorer's [phishing filter](#) offers the best service in this space, Moyer says. Microsoft does take public submissions, but mostly relies on privately fed data to create this list and [Google](#) relies purely on public crowd-sourcing to create its list.

"Both only identified a fraction of our sample set" of malware, Moyer says. "This is at best a stop-gap measure."

While Accuvant didn't declare a winner in its browser security testing, it did praise a competitive browser market for improving security overall. "Every company is trying to make their browser a little bit better than their competitors, and the result is everyone gets better over time," Mehta says.

Accuvant will release a full study that includes other aspects of browser security soon.

Brian Jackson Brian Jackson is the Associate Editor at ITBusiness.ca. Follow him on [Twitter](#), read his [blog](#), and check out the [IT Business Facebook Page](#).

[Print](#)

[Close Window](#)