Report: Using silent updates boosts browser security

by Steve Ragan - May 4 2009, 17:00

Using silent updates boosts browser security report says. (IMG:J.Anderson)

1 | 2

In a recent report from Google Switzerland and the ETH (Swiss Federal Institute of Technology) in Zurich, Google Web server logs were analyzed in order to compare and rank update strategies used by Chrome, Firefox, Opera, Safari, and Internet Explorer.

The overall conclusion of the data collected shows that silent updates are the best way to ensure end users are on the most recent version of any given browser, which ultimately leads to mitigation of client-side vulnerabilities where the browser is the delivery vehicle.

The report, written by Thomas Duebendorfer and Stefan Frei, is a follow-up of sorts to a browser security report released earlier this year, and also one from Defcon in 2008.

The previous report, from Defcon, centered on the findings that over 45 percent of the users who visited Google Web servers were not using the most recent version of their browser at the time. The new research examines the update methods used by the browsers online today and, for the first time, includes Google’s Chrome.

Using the most recent version of a browser will lower the risk associated with drive-by-downloads and other Web-based attacks, which start by targeting the browser. In the 2008 report, Firefox was the browser that offered the best security protection by using the most effective update strategy of any popular browser.

Yet in their recent paper, Duebendorfer and Frei said they wanted to expand on previous research.

“We were wondering if one cannot do even better than Mozilla Firefox by deploying a different update mechanism in a Web browser. The Google Chrome Web browser… is using a so-called silent update mechanism. The user currently cannot disable auto-updates in Google Chrome, which is different from any other browser update mechanism in use today," they wrote.

"This gave us a great opportunity to evaluate the effectiveness of Google Chrome's update mechanism by comparing it to other Web browsers using the same data source and a similar measurement methodology as used in our two previous Web browser studies."

When you break down the various update measures, as the researchers did, clearly Google wins hands down. Chrome will look for an update every five hours, and download and install it without informing the user. According to the paper, as of April 2009, the user has no control over this process, cannot disable the updates and, in most cases, a browser restart isn't needed.

By way of contrast, Firefox, Safari, Opera, and Internet Explorer offer various levels of update control. Firefox allows manual update checking, as well as an automatic check for updates when appropriate. In addition, using 'about:config' allows for more granular update control and the ability to disable updates.

Safari, using an update service similar to Google's, but offering the ability to disable it and control the frequency of checks for new versions, lacks the ability to discover new updates instantly. This is because Safari only looks for new versions based on what the user allows -- this schedule being daily, weekly, monthly, or not at all. If the check has been performed, and a new version becomes available afterwards, then the user will only see an alert during the next scheduled check.

Opera, using a fixed 'once per week' schedule for updates, offers no control to the end user and, according to the report, will force a complete reinstall of the browser to apply the update. This, in addition to the many steps required by the user when they update, means most Opera users are often behind in patching. Opera 10, the newest release currently in testing, will update automatically once a new version is released. This will lower the steps needed to update, but still leaves little control with the user.

Lastly, Internet Explorer will receive updates and patches by using Windows Update services. The patches are pushed monthly if needed, and the user can control them by configuring Window's Automatic Update settings. The problem with this, the researchers say, is that businesses often use an internal Windows Update server, pushing patches and fixes on their own schedule. This leaves the end user vulnerable by using an out-of-date browser until the patches are pushed internally.

Based on the data collected, 97 percent of Chrome users were running the current release within 21 days (at the time the release version was 1.0.154.48), Firefox users hit a high of 85 percent within 21 days of version 3.0.8, Safari users with version 3.1.x earned a maximum of 53 percent, while those on 3.2.x faired considerably lower in rank.

The reason for this, according to the report, is that: "Apple put the bar higher to who is eligible for updates to Apple Safari 3.2.x by requiring Mac OS X Tiger 10.4.11 or higher or Mac OS X Leopard 10.5.5 or higher with Security Update 2008-007 installed. Given that Apple Safari 3.2.1 reaches only [33 percent] on day 21 after release, that's an additional [20 percent] of Apple Safari 3.x users that were left behind since Apple Safari 3.2.x came out."

"It's not the first time that installation requirements prevent users from updating browsers: users of OS X Panther 10.3, the most recent OS X until OS X Tiger 10.4 was released on April 29, 2005, are limited to Apple Safari 1.3 and Mozilla Firefox 2. Similarly, Windows 9x users have to stick with Mozilla Firefox 2 and Microsoft Internet Explorer 6 and Win 2000 users are limited to Microsoft Internet Explorer 6, the effect of which is measured in," the report added.

Overall, Opera scored the lowest of the tested browsers. Three weeks after a new release, only 24 percent of Opera users were updated to the newest version.

“It's a pity that 76% of Opera 9.x users currently don't benefit from the security improvements and new features of new Opera versions within three weeks of its release. If some engineering time were spent on increasing update effectiveness instead of working on new features, this would eventually benefit many more users,” the report said, adding that the overall poor effectiveness of Opera and Safari’s update schemes gives plenty of time for attackers to exploit the browsers to attack end-user systems.

As for Internet Explorer, because there is no minor versioning within the browser, the researchers were unable to verify the update speed of those who use it, noting: “The often stated reason for this omission is to reduce information leakage and make it harder for an attacker to select a working exploit for the actual browser version in use. As we have seen drive-by download Web sites trying many different exploits at once, it's unclear how much additional protection this omission really gives.”

1 | 2

- Email
- RSS
- Talkback

- Delicious
- Digg
- FARK
- Slashdot
- StumbleUpon

vote now

Talkback

There are currently no comments for this article. Be the first to comment! (no registration required)

Security
Index
News

Features

Using silent updates boosts browser security report says. (IMG:J.Anderson)

1 | 2

Again, using the most recent version of any given browser will help address several layers of security and mitigate some levels of attack. There is no arguing against this. However, the issue of control is still something that security professionals and software vendors struggle with.

Is it right to remove control from the end user? As you can see when looking at how Firefox, Internet Explorer, Safari, and Opera control updates, the vendors think the end user needs to have some level of control when it comes to installing new versions of the software.

Moreover, despite the security risks, some users choose to ignore the updates. This can be for several reasons, but ultimately it's a conscious decision on their part. This level of 'give and take' comes in all software and not just browsers. In most cases, a user will need to search for an update and actively install it. Even if the software offers an update alert, the user must take steps when updating it.

On the other side of the argument, security professionals claim that Google's method of updating Chrome is a perfect solution for end users who either choose to ignore updates, or those who don't understand the risks of not applying patches. It's often said that someone who doesn't apply a security patch not only places themselves at risk, but others as well.

This is true, but there is a fine line when it comes to controlling a vendor's software and the rights an end user has over it. Is it worth crossing those lines or risking their crossing by removing the control from all users, even those who understand the risks, in an effort to protect the minority of end users who are at risk unwillingly or by their own choice?

Sadly, while the idea is nice, end users *should* have control over their systems. Chrome's instant update feature is amazing, and should be adopted by all browsers. Perhaps a good plan is one that meets the needs of the security-conscious person and average user by offering a compromise.

One such compromise would be the option for the user to upgrade now -- in-place -- with little action and no browser restart, combined with a warning or requirement that the patch needs to be installed within 21 days.

Moreover, if the patch is urgent, as determined by the vendor using a standard of risk assessment (which looks at the vulnerability type) users who would be affected, the odds of them being successfully exploited with little or no interaction, and the severity of exploitation -- such as preventing a Malware outbreak like Conficker -- then the patch is instant and everyone gets it, no matter what.

The report by Duebendorfer and Frei does an excellent job of breaking down the risks involved by not patching browsers with current releases, and explaining how each of the popular platforms addresses end-user control over the patching process. In addition, they comment on the predictable nature of the patch cycles used by Microsoft, calling it 'suboptimal' for patches to Internet Explorer to remain on a fixed cycle based on demand by business customers.

“A fixed patch schedule mainly benefits the patch management processes of larger corporations... Based on our measurements and the evolution of the threats towards end-users we suggest that software vendors release patches for attack exposed applications, such as Web browsers and plug-ins, as soon as they are available... We believe that there is room for a better trade-off to benefit overall security,” the report commented.

Yet, that trade-off applies not just to patch cycles from a vendor, but to the end user as well. Some users want that trade-off, and while Google does an excellent job of ensuring Chrome users are promptly patched against security issues, they remove the trade-off by stripping the user of overall control.

At the end of the day, while the report certainly covers the bases of risk mitigation and explains how each browser deals with updates, the only way to adequately defend against online threats that use the browser as an attack surface is to patch constantly and consistently. It doesn’t matter which browser you use, as long as you are consistent in updating it.

The struggle to get everyone to update faster is one that will remain for a long time and, for the most part, vendors will always fight with this because they refuse to remove the control from the user. For them, that's a trade-off on its own, as Mozilla, Microsoft, Opera, and Apple would rather leave the patch in the hands of the user rather than force something on them and risk taking heat over it.

If anything, Google can be commended on at least taking a stance, even if it removed control, because it's pushing updates and keeping the overwhelming majority of its users on the same browser version. Google may be criticised over this decision, yet that was the trade-off, and one it was willing to make.

The complete research can be viewed online by clicking here.

1 | 2