Mozilla Firefox Exploit
10 Aug 2015

We have been made aware of a recently discovered vulnerability in Mozilla Firefox. The announcement from Mozilla can be found at https://blog.mozilla.org/security/2015/08/06/firefox-exploit-found-in-the-wild/ and reads:

> Yesterday morning, August 5, a Firefox user informed us that an advertisement on a news site in Russia was serving a Firefox exploit that searched for sensitive files and uploaded them to a server that appears to be in Ukraine. This morning Mozilla released security updates that fix the vulnerability. All Firefox users are urged to update to Firefox 39.0.3. The fix has also been shipped in Firefox ESR 38.1.1.
>
> The vulnerability comes from the interaction of the mechanism that enforces JavaScript context separation (the "same origin policy") and Firefox's PDF Viewer. Mozilla products that don't contain the PDF Viewer, such as Firefox for Android, are not vulnerable. The vulnerability does not enable the execution of arbitrary code but the exploit was able to inject a JavaScript payload into the local file context. This allowed it to search for and upload potentially sensitive local files.
>
> The files it was looking for were surprisingly developer focused for an exploit launched on a general audience news site, though of course we don't know where else the malicious ad might have been deployed. On Windows the exploit looked for subversion, s3browser, and Filezilla configurations files, `.purple` and Psi+ account information, and site configuration files from eight different popular FTP clients. On Linux the exploit goes after the usual global configuration files like `/etc/passwd`, and then in all the user directories it can access it looks for `.bash_history`, `.mysql_history`, `.pgsql_history`, `.ssh` configuration files and keys, configuration files for remina, Filezilla, and Psi+, text files with "pass" and "access" in the names, and any shell scripts. Mac users are not targeted by this particular exploit but would not be immune should someone create a different payload.
>
> The exploit leaves no trace it has been run on the local machine. If you use Firefox on Windows or Linux it would be prudent to change any passwords and keys found in the above-mentioned files if you use the associated programs. People who use ad-blocking software may have been protected from this exploit depending on the software and specific filters being used.

We recommend that anyone using the Mozilla Firefox browser should perform an update, as suggested above. The best way to do this, according to Mozilla, is to click on the **Help** tab in your menu and then selecting **Check for updates**.