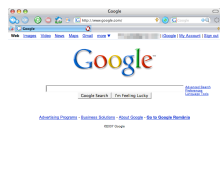


12 November 2007

By: Bogdan Popa, Security and Search Engines Editor



Mozilla Firefox

## [Firefox Security Flaw Affecting Gmail's Users](#)

### *The Firefox JAR vulnerability still there*

Last week, security companies around the world spotted a new vulnerability in Mozilla Firefox which could allow the attackers to use a malicious JAR file to harm users' computers. The security flaw is still there and moreover, it seems it affects most websites on the Internet including the super search giant Google. GnuCitizen wrote that Michal Zalewski from Google (you know, that famous hacker who joined Googleplex) required additional information about a potential exploitation over the company's technologies. In addition, beford.org discovered a way to steal the Gmail contact list using a malicious JAR file especially created to take advantage of the Firefox vulnerability. I'm not going to offer you more details about it but I'll give you a tip on how to remain protected against attacks. You can always install the NoScript extension which was already updated to provide protection for this exploit. In case you never tried it, NoScript is an add-on designed to work with Mozilla Firefox which is supposed to disable the webscripts included on the websites you choose. Obviously, you can always choose another browser to visit the Internet pages which will surely keep you away from the Firefox JAR attacks. But in case you're a Firefox-addicted user, I think you can try signing out of your account but I'm not sure this would be 100 percent efficient. However, stay away from dangerous websites and unknown links which could attempt to steal your private Google information. Now, since the flaw affects both Google and Firefox, I'm pretty curious to see which will be the first company to patch it. "Who's fault? Both, Google for having open redirect issues and not fixing them, and Mozilla Corporation for failing to address this problem," beford wrote. You can download the latest version of Firefox straight from [Softpedia](#).