

16 January 2007

By: Bogdan Popa, Security and Search Engines Editor



ANOTHER GOOGLE SECURITY FLAW!

It seems like Google's services are more and more vulnerable

Because Google is a company that provides a huge number of online solutions, it was often avoided by viruses, security flaws and vulnerabilities. Recently, the company was affected by multiple security holes that made Google's users vulnerable to attacks. One of the most known vulnerabilities concerns Gmail and it was able to allow an attacker to view your entire contact list. Last week, Google Blogoscoped posted a detailed article on their blog to announce a new security hole in the company's services that can permit an attacker to read the subject of the e-mails stored in your Gmail account, view the feeds added in Google Reader and read your entire private Notebook. Yesterday, Philipp Lenssen announced that Google sent him a message saying that the company fixed the flaw and users are now safe. Today, Google Blogoscoped published a new article to announce another security flaw in Google's service that can allow an attacker to read your Gmail messages' subjects, access and modify Google Docs & Spreadsheets and even view your search history. "Hard to believe but true: there's another vulnerability currently live on Google's servers, allowing a malicious hacker to point you to a (long) Google.com URL... and then receive your cookie data, with which the hacker can access and modify your Google docs and spreadsheets, and view your email subjects & first words, your search history (if enabled) and much more... similar to the previous vulnerability," Philipp Lenssen said. It seems like the vulnerability concerns a Google service that isn't able to defend against HTML exploits so an attacker can use this vulnerability to access all your Google services through this solution. Philipp refused to publish additional details about the flaw to avoid unwanted exploitations of the vulnerability. "This particular security hole is connected to an update to a specific Google service which doesn't correctly defend against HTML injections, leading to the ability to JavaScript-write something which passes cookie data to an external source. I won't reveal the details here for now and rather give Google time to fix this bug - Haochi of Googlified alerted their security team 7 hours ago," he added. The Blogger also mentioned that no user can be affected if they refuse to click on a malicious weblink, no matter if it belongs to Google or not, so it's safer to visit only secure websites. It seems like Google repaired the issue and the HTML injection is now correctly defended by the services provided by the search giant.