

15 January 2007

By: Bogdan Popa, Security and Search Engines Editor



## [The Critical Google Security Hole Was Fixed](#)

### *No more account hijacking*

Google Base, Docs & Spreadsheets, Calendar, Gmail, Google Talk, Reader, Blogger, YouTube, Video, Search Engine, University Search, Book Search, Government Search and many, many other services. All these solutions are making Google the most powerful company in the entire world. As you know, the search giant is challenged every day by its rivals with new products but it seems like the company was meant to be the leader of the online solutions. For example, multiple companies are currently offering service that allows you to publish and share your video files with other members of the community. That's why Google decided to acquire YouTube, one of the most popular solutions in its category, and updated it to make the solution even more powerful. Because Google is an online company, the company was often avoided by viruses, vulnerabilities and other kinds of security issues. Although it provides a big number of online solutions, Google was recently affected by multiple security flaws that made Google's users vulnerable to attacks and exploits. As an example, I can mention the Gmail issue that enabled an attacker to see your entire contact list after you visited a malicious site. Then, the company announced that almost 60 users reported that they found their Gmail's inbox empty without any e-mail message sent or received. So, no matter what company provides the service you use, it's obvious that you can be vulnerable anytime. This fact is also sustained by a new vulnerability identified in Google services that can allow an attacker to view your information from ALL solutions provided by the search giant. Tony Ruscoe found an issue in Google's accounts that can enable you to view documents in Google Docs & Spreadsheets, read e-mails' subject stored in Gmail's inbox, view Google account page and your private Notebook and also enter the Google Reader account. Philipp Lenssen from Google Blogoscoped said that Google was informed by the existence of the issue and he will publish more information after the company will fix the flaw. Today, the search giant announced the blogger that the security issue was fixed after almost a week since the company received the feedback messages. "I've now received confirmation from Google's Security Team that the latest vulnerability Philipp posted about has been fixed. After carrying out some investigations of my own, I believe this is the case - so I'm going to share with you what the problem was and how I was able to exploit it. In doing so, I hope to educate other developers about the potential flaws that can occur in growingly complex web applications," Philipp said. "In summary, I was able to create a page that was hosted on a google.com domain, which is something that should never be allowed to happen. Because of this vulnerability, I was then able to use a simple bit of code to steal someone else's Google cookie and access their Google services," he said about the exploitation of the vulnerability.