

# [VulnWatch] Overtaking Google Desktop

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2007-02/msg00017.html>

---

- *From:* "Yair Amit" <[yairam\\_ng@xxxxxxxxxxxxxx](mailto:yairam_ng@xxxxxxxxxxxxxx)>
  - *Date:* Wed, 21 Feb 2007 16:06:58 +0200
- 

Hello,

A new research from Watchfire has revealed a serious vulnerability in Google Desktop.

The attack, which is fully presented in a new Watchfire research paper released today (available at <http://www.watchfire.com/resources/Overtaking-Google-Desktop.pdf>), can allow a malicious individual to achieve not only remote, persistent access to sensitive data, but in some cases full system control as well.

Google Desktop is a popular freeware desktop search tool which offers powerful indexing abilities along with an easy to use interface. In many cases, Google Desktop manages highly sensitive information. Therefore, the impact of a security breach in it is far-reaching.

Google Desktop contains several protection mechanisms to secure its indexed data against remote intruders.

In this paper, we present a step-by-step attack flow that circumvents Google Desktop's protection mechanisms and allows a malicious attack to take place against Google Desktop users.

The attack is composed of web-application security flaws found in Google Desktop along with exploitation of Google Desktop's tight integration with the Google.com website.

The paper shows that it is possible to achieve a remote and persistent access to sensitive data on attacked systems.

In addition, under certain conditions, it is also possible to covertly inject and execute malicious applications on attacked systems, using Google Desktop's own features.

The full paper can be found in the following link:

<http://www.watchfire.com/resources/Overtaking-Google-Desktop.pdf>

A demonstration of the attack flow can be found at the same page or at the following link:

<http://download.watchfire.com/googledesktopdemo/index.htm>

## [VulnWatch] Overtaking Google Desktop

Note:

-----  
The Google Desktop security flaw was coordinated with the Google Security Team.

Google has been responsive and recently issued a patch which mitigates the risk of the attack.

We highly recommend all Google Desktop users to make sure they have an updated version installed on their system.

This vulnerability was discovered by me with the cooperation of Danny Allan and Adi Sharabani.

Best regards,  
Yair Amit  
Security Team  
Watchfire (Israel) Ltd.