

# Google Desktop Cracked

Monday, 11 September 2006

Last Updated Saturday, 16 February 2008

## Google Desktop Cracked

An unpatched design flaw in Microsoft Corp.'s Internet Explorer browser could give malicious hackers an easy way to use the Google Desktop application to covertly hijack user information. Matan Gillon, a hacker from Israel, discovered the vulnerability in the cross-domain protections in Internet Explorer and published a proof-of-concept exploit to show how Google Desktop can be cracked.

"The proof of concept works on a fully patched IE browser (default security and privacy settings) with Google Desktop v2 installed," Gillon said in a note sent to Ziff Davis Internet News.

He also published a detailed explanation of the vulnerability and warned that an attacker simply needs to lure a target to visit a malicious Web page. "Much like classic XSS (cross site scripting) holes, this design flaw in IE allows an attacker to retrieve private user data or execute operations on the [user's] behalf on remote domains," Gillon explained.

A spokeswoman for Microsoft acknowledged the flaw in a statement and said the company was unaware of active attacks against IE users.

"This issue could potentially allow an attacker to access content in a separate Web site if that Web site is in a specific configuration," the spokeswoman said, adding that Microsoft is working on a fix. The company may also release a security advisory to provide temporary mitigation guidance.

The bug is described as a design flaw that causes IE to allow a violation of the cross-domain security model. Gillon explained that IE does not properly parse CSS (cascading style sheet) files and allows the importation of files that are not valid CSS files.

This opens the door for attackers to disclose HTML and script code from the remote site that was improperly imported as a CSS file. This site may exist in another domain than the site that exploits the issue.

Gillon used the Google Desktop utility to prove his findings, but in theory, any domain or application that depends on the IE cross-domain security model is vulnerable.

"Thousands of Web sites can be exploited, and there isn't a simple solution against this attack at least until IE is fixed," Gillon said.

[Click here](#) to more about another unpatched IE vulnerability.

Google spokeswoman Sonya Boralv said initial investigations show that the problem resides in IE and not as a result of any vulnerabilities in Google Desktop, the downloadable utility that lets PC users merge desktop and search results on the well-known browser interface.

"Google takes the security of its users very seriously. We just learned of this issue and are looking into it," Boralv said.

Gillon said he tested the issue on alternative browsers and found that Mozilla Firefox seems to adequately keep domain restrictions in CSS imports and doesn't seem to be vulnerable to this type of attack. "Opera isn't vulnerable because it doesn't support the style sheets collection," he added.

As a temporary solution, he recommends that IE users disable JavaScript or use a different browser.

Check out eWEEK.com's Security Center for the latest security news, reviews and analysis. And for insights on security coverage around the Web, take a look at eWEEK.com Security Center Editor Larry Seltzer's Weblog.