

Advisory : Google-Orkut Link Traversing Bug.

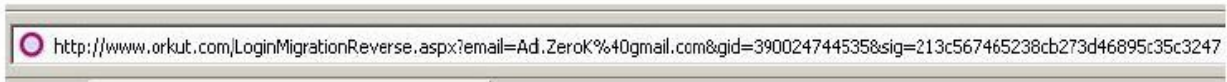
Dated : 1 September 2006

Severity : Critical

By: Aditya K Sood [<http://www.secniche.org>]

Explanation:

A specific bug proliferates when a gmail account is linked to orkut account. There is a specific group ID is provided to every account and a signature ID which is the cause of worry. The hacker can easily manipulate it and do very erroneous linking with the wrong user Ids of its own choice. The email even gets manipulated as no check is present and the page is uploaded as :



One can see email with gid and sig. There is no check is present. The attacker can easily change the email id as:



The output is :



The rogue linking is possible though this. It enable attacker to launch phishing attacks and manipulative linking between the gmail and orkut accounts. Fake linking is possible. The attacker can infect large number of users.

Response:

**Date:** [Fri, 08 Sep 2006 13:51:03 -0700](#)

**Subject:** Re: [#72460488] Link Travesing bug.[ Explanation PDF]

[This is Spam](#) | [Block Sender](#) | [Full Header](#)

Hi Aditya,

Thanks for bringing this to our attention. We're sorry to hear about the problem you are experiencing and are currently investigating this situation. We appreciate your vigilance and hope to keep orkut.com a safe, trusted community.

We're always interested in hiring bright, talented individuals who are passionate about the seemingly infinite task of organizing the world's information and making it universally accessible. To learn about opportunities currently available at Google, please visit our Jobs page at

<http://www.google.com/jobs/>.

To apply for openings that interest you, please send your resume to [jobs@google.com](mailto:jobs@google.com).

Stay beautiful,  
orkut.com

Vendor Status : Reported and Patched.