

# [VulnWatch] Orkut Email Address Disclosure Vulnerability

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2006-12/msg00006.html>

---

- *From:* Rajesh Sethumadhavan <[rajesh.sethumadhavan@xxxxxxxxx](mailto:rajesh.sethumadhavan@xxxxxxxxx)>
  - *Date:* Thu, 7 Dec 2006 13:08:27 -0800 (PST)
- 

## Orkut Email Address Disclosure Vulnerability

```
#####  
XDisclose Advisory : XD100097  
Vulnerability Discovered: November 30th 2006  
Advisory Released : December 8th 2006  
Credit : Rajesh Sethumadhavan  
Class : Information Disclosure  
Severity : Highly Critical  
Solution Status : Unpatched  
Vendor : Google Inc  
Vendor Website : http://www.orkut.com  
Affected applications : Orkut Services  
Affected Platform : All  
#####
```

### Overview:

Orkut is an Internet social network service run by Google and named after its creator, Orkut Büyükkökten. It claims to be designed to help users meet new friends and maintain existing relationships with pictures and messages, and establish new ones by reaching out to people you've never met before.

Orkut service is vulnerable to email address disclosure vulnerabilities. Due to this It is possible to get email address of any users in orkut. This is caused due to improper designing of orkut portal.

### Description:

A remote attacker can get the email address of anyone in the orkut as demonstrated below. The victim interaction is not required at all.

### Demonstration:

- Note: Demonstration leads to email address information disclosure
- Login to your orkut account
  - Add any user as your friend (Person you want to get email address)
  - Click 'friends' tab
  - Click 'open friend requests' tab
  - Click edit button the email address of the user will be displayed

## [VulnWatch] Orkut Email Address Disclosure Vulnerability

as in the screenshot

Same way your can find your friends email address also

Solution:

Orkut can improve their portal design by hiding the users email address

Screenshot:

<http://www.xdisclose.com/images/xdorkutemailid.jpg>

Impact:

Successful exploitation allows email address disclosure.

Original Advisory:

<http://www.xdisclose.com/XD100097.txt>

Credits:

Rajesh Sethumadhavan has been credited with the discovery of this vulnerability

Disclaimer:

This entire document is strictly for educational, testing and demonstrating purpose only. Modification use and/or publishing this information is entirely on your own risk. The exploit code is to be used on your own orkut account. I am not liable for any direct or indirect damages caused as a result of using the information or demonstrations provided in any part of this advisory.

---

Any questions? Get answers on any topic at Yahoo! Answers. Try it now.