

# Re: [VulnWatch] IMail Account hijack through the Web Interface

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2002-03/0162.html>

---

**From:** Zillion ([zillion@safemode.org](mailto:zillion@safemode.org))

**Date:** 03/11/02

Date: Mon, 11 Mar 2002 04:11:43 +0000 (GMT)

From: Zillion <[zillion@safemode.org](mailto:zillion@safemode.org)>

To: Obscure <[obscure@zero6.net](mailto:obscure@zero6.net)>

Hi all,

I think this was already covered for Imail 7.04 in the following advisory:

<http://cert.uni-stuttgart.de/archive/bugtraq/2001/10/msg00082.html>

The workaround given by Ipswitch was:

Turn off the "ignore source address in security check" option. This isn't a bullet proof workaround (think of proxies,nat etc) but can help to prevent abuse of this issue.

zillion

On Sun, 10 Mar 2002, Obscure wrote:

- > *Advisory Title: IMail Account hijack through the Web Interface*
- > *Release Date: 10/03/2002*
- > *Application: IMail Server*
- >
- > *Platform: Windows NT4*
- > *Windows 2000*
- > *Windows XP*
- >
- > *Version: 7.05 or earlier*
- >
- > *Severity: Malicious users can easily access other people's accounts.*
- >
- > *Author: Obscure^ [ [obscure@eyeonsecurity.net](mailto:obscure@eyeonsecurity.net) ]*
- >
- > *Vendor Status: Informed on 21 Feb 2002, a fix was already issued to*
- > *customers.*
- >

## SecurityFocus Bugtraq: Re: [VulnWatch] IMail Account hijack through the Web Interface

- >
- > *Web:*
- >
- > <http://www.eyeonsecurity.net>
- > <http://www.ipswitch.com>
- >
- >
- >
- > *Background.*
- >
- > *(extracted from*
- > [http://www.ipswitch.com/Products/IMail\\_Server/index.html](http://www.ipswitch.com/Products/IMail_Server/index.html))
- >
- > *The 20–Minute E–Mail Solution.*
- > *IMail Server is an easy–to–use, web–enabled, secure and*
- > *spam–resistant*
- > *mail server for Windows NT/2000/XP. It is the choice*
- > *of businesses, schools, and service providers.*
- >
- > *A Great Price–Performer.*
- > *Unlike Microsoft® Exchange and Lotus® Notes, which are costly to*
- > *deploy and cumbersome to administer, IMail Server is easy*
- > *to install and easy to manage. It has a simple pricing structure and*
- > *is scalable to thousands of users per server.*
- >
- >
- > *Problem.*
- >
- > *When a user logs in to his account through the Web interface, the*
- > *session authentication is maintained via a unique URL.*
- > *By sending an html e–mail which includes an image at another server,*
- > *an attacker can easily get the unique URL via the*
- > *referer field in the HTTP header.*
- >
- >
- > *Exploit Example.*
- >
- > <http://eyeonsecurity.net/tools/referer.html>
- > *A CGI script sends an e–mail with an attached image, pointing to*
- > *another CGI script which sends the referer URL to the*
- > *attacker.*
- >
- >
- > *Fix*
- >
- > *Upgrade to IMail 7.06. The fixed version checks for the IP. The*
- > *authentication now relies on the unique URL and the IP*
- > *address. Of course users who log in to IMail Web interface from*
- > *behind*
- > *proxies, are still vulnerable.*
- >

SecurityFocus Bugtraq: Re: [VulnWatch] IMail Account hijack through the Web Interface

>  
> *ps. this same vulnerability effects Excite WebMail. The Excite guys*  
> *did not contact me back.*  
>  
>  
> *Disclaimer.*  
>  
> *The information within this document may change without notice. Use*  
> *of*  
> *this information constitutes acceptance for use in an AS IS*  
> *condition. There are NO warranties with regard to this information.*  
> *In no event shall the author be liable for any consequences*  
> *whatsoever*  
> *arising out of or in connection with the use or spread of this*  
> *information. Any use of this information lays within the user's*  
> *responsibility.*  
>  
>  
> *Feedback.*  
>  
> *Please send suggestions, updates, and comments to:*  
>  
> *Eye on Security*  
> *mail : [obscure@eyeonsecurity.net](mailto:obscure@eyeonsecurity.net)*  
> *web : <http://www.eyeonsecurity.net>*  
>  
>

- 
- ***Previous message:*** [Obscure: "IMail Account hijack through the Web Interface"](#)
  - ***In reply to:*** [Obscure: "IMail Account hijack through the Web Interface"](#)
  - ***Next in thread:*** [Obscure: "Re\[2\]: \[VulnWatch\] IMail Account hijack through the Web Interface"](#)
  - ***Next in thread:*** [Henrik Larsson: "Re: IMail Account hijack through the Web Interface"](#)
  - ***Reply:*** [Obscure: "Re\[2\]: \[VulnWatch\] IMail Account hijack through the Web Interface"](#)
  - ***Messages sorted by:*** [\[ date \] \[ thread \] \[ subject \] \[ author \] \[ attachment \]](#)