security-assessment.com

Vulnerability Advisory

Name	RockLiffe MailSite Express WebMail
Vendor Website	http://www.rockliffe.com/products/express-webmail-server.asp
Date Released	October 28, 2005
Affected Software	RockLiffe MailSite Express WebMail prior v6.1.22
Researcher	Paul Craig : paul.craig@security-assessment.com

Description

"For those companies that want to create their own site that hosts hundreds of thousands to millions of web based email users, MailSite Express is the answer."

During an audit of a client, Security-Assessment.com discovered multiple critical vulnerabilities within the RockLiffe MailSite Express WebMail software.

Exploitation

- **Exploit 1: Cross Site Scripting Vulnerabilities**

Recipients who save their login information locally are vulnerable to account theft when viewing HTML encoded messages with embedded JavaScript.

When the option to save login information is selected, a user's password is stored as plaintext within the cookie.

Crafting an email with scripting in the body will cause the execution of the scripting in the context of the site, allowing for the theft of the stored credentials.

- A basic test for this is to include the following in the body of a message;
  <script> alert(document.cookie) </script>

- **Exploit 2: Multiple Script Attachment Validation Flaws**

The WebMail software attempts to verify the validity of an attachment within a received message. Security checks will automatically modify the extension of any attached files ending in .asp, changing them to .asp.txt. This is an attempt to avoid remote code execution through an attached file.

However, these validity checks can be defeated and script files saved to the server.

By default, only files ending in .asp are identified and rejected as script files. If a malicious user were to attach an .asa file instead, WebMail would accept the script attachment, saving the file locally with the .asa extension.

When the .asa file is requested the script contents are executed in the same manner as a .asp file. This flaw could also be affected by other extensions such as .htr and .aspx.

A similar flaw exists when an attachment is sent with the filename unknown.unk.

In this instance the message subject is used as the file name, and .asa script files can be saved locally.

- **Exploit 3: Retrieve Arbitrary System Files via Web Mail**

The location of file attachments for a mail message currently been composed, are stored as a physical file path included in the HTML as a hidden field.

An example of this is shown below;

- <input type="hidden" name="AttachPath"
  value="H:\Express3Webmail6.1.20\cache\5116FC5113B47C0B1CDD5\440820634>

This value points to the location where the attachments for the message are stored, by default all files within this directory are considered attachments for the message currently being composed.

This value can be manipulated and a message can be sent with arbitrary 'attachments'.

- For example, posting the variable AttachPath = H:\Express3Webmail6.1.20\ would send the recipient a copy of the docroot.

Solution

- Security-Assessment.com has been in contact with RockLiffe software and a new version of the software has been released to address the discovered vulnerabilities.

  Security-Assessment.com urges RockLiffe users to upgrade to v6.1.22 by downloading the new version at http://www.rockliffe.com/userroom/download.asp

About Security-Assessment.com

Security-Assessment.com is a leader in intrusion testing and security code review, and leads the world with SA-ISO, online ISO17799 compliance management solution. Security-Assessment.com is committed to security research and development, and its team have previously identified a number of vulnerabilities in public and private software vendors products.

For further information on this issue or any of our service offerings, contact us

Web www.security-assessment.com
Email info@security-assessment.com
Phone +649 302 5093