

[NT] SurgeMail Webmail Multiple Vulnerabilities (Directory Traversal, Cross Site Scripting)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-03/0128.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 03/28/05

To: list@securiteam.com

Date: 28 Mar 2005 10:28:02 +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>

SurgeMail Webmail Multiple Vulnerabilities (Directory Traversal, Cross Site Scripting)

SUMMARY

<<http://netwinsite.com/surgemail/>> SurgeMail is a next generation Mail Server – Combining features, performance and ease of use into a single integrated product. Ideal on Windows NT/2K, or UNIX (Linux, Solaris etc) and supports all the standard protocols IMAP, POP3, SMTP, SSL, ESMTP.

Two vulnerability were found in SurgeMail's Webmail, one in the file attachment upload feature and the other in the auto-reply feature. These vulnerabilities may be exploited by a malicious Webmail user to upload files to certain locations on the server, obtain file listings of certain directories, send certain files on the server to him/herself and/or place a JavaScript code inside an auto-replay feature in the Header and subject input fields.

DETAILS

Vulnerable Systems:

- * SurgeMail version 2.2g3

Securiteam: [NT] SurgeMail Webmail Multiple Vulnerabilities (Directory Traversal, Cross Site Scripting)

Immune Systems:

* SurgeMail version 3.0c2

Directory Traversal:

SurgeMail allows a logged user to attach files when composing a new email via the Webmail interface.

The uploaded file is temporarily stored in the

c:\surgemail\web_work\u_xx\xxxx@hostname@hostname\attach\RandomNumber\ directory. In particular, the value of SomeRandomNumber is part of this POST request (attach_id parameter) and is under the attacker's control.

The server will create the directory "RandomNumber" if it does not exist.

By using directory traversal characters, it is possible to cause the uploaded files to be written to directories that reside outside the attach subdirectory.

Cross Site Scripting:

A user is allowed to configure an email auto-reply message using the Webmail interface. This auto-reply message consist of a message subject and a message header. It is possible to inject JavaScript in both these fields. If the Webmail administrator views this user's auto-reply message settings, the injected JavaScript will be executed on his browser. This may be exploited by a malicious user to steal the Webmail administrator's cookies or to redirect the administrator's browser to malicious websites.

Another XSS vulnerability occurs when webmail.exe is displaying an error message in response to an invalid value in the page parameter. The error message also reveals the installation path.

Workaround:

Please update to the latest version of SurgeMail Webmail.

Disclosure Timeline:

18 Mar 05 – Vulnerability Discovered
19 Mar 05 – Vulnerability Verification
19 Mar 05 – Initial Vendor Notification
22 Mar 05 – Vendor replied with fixed version
23 Mar 05 – Public Release

ADDITIONAL INFORMATION

The information has been provided by <mailto:chewkeong@security.org.sg> chewkeong.

The original article can be found at:

<<http://www.security.org.sg/vuln/surgemail22g3.html>>
<http://www.security.org.sg/vuln/surgemail22g3.html>

=====

Securiteam: [NT] SurgeMail Webmail Multiple Vulnerabilities (Directory Traversal, Cross Site Scripting)

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.