

[NT] RockLiffe MailSite XSS and DoS

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-01/msg00084.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxx>
 - *Date:* 25 Jan 2006 09:56:04 +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>

RockLiffe MailSite XSS and DoS

SUMMARY

" <<http://www.rockliffe.com/>> Rockliffe's MailSite is a program for providing access to email accounts on Microsoft Windows operating systems." MailSite HTTP Mail management agent allows a remote attacker to cause a denial of service or execute arbitrary script code.

DETAILS

Vulnerable Systems:

- * MailSite version 7.0.3.1 and prior
- * MailSite version 6.1.22 and prior
- * MailSite version 5.x

MailSite HTTP Mail management agent version 7.0.3.1 allow a remote attacker cause a denial of service. The bug exists in the input validation routine of httpma that causes the svchost process to consume CPU cycles and impacting MailSite HTTP Management agent that will ultimately crash the service.

The MailSite HTTP Mail management agent versions 6.x and 5.x allows a remote attacker to inject arbitrary script code. This vulnerability is

[NT] RockLiffe MailSite XSS and DoS

caused due to a design error in the wconsole.dll. This dll file contains html code embedded in it which is not properly sanitizing the user-input.

Proof of Concept:

For 7.x series

[http://\[website\]:90/CGI-BIN/WCONSOLE.DLL?Authenticate|cmd](http://[website]:90/CGI-BIN/WCONSOLE.DLL?Authenticate|cmd)

Any special characters passed to the parameters in the wconsole.dll triggers denial of service.

For 6.x & 5.x series

[http://\[website\]:90/CGI-BIN/WCONSOLE.DLL?%3Cscript%3Ealert\(document.cookie\)%3C/script%3E](http://[website]:90/CGI-BIN/WCONSOLE.DLL?%3Cscript%3Ealert(document.cookie)%3C/script%3E)

Vendor Status:

The vendor has issued a fix:

For 7.x series apply the following patch:

<ftp://ftp.rockliffe.com/MailSite/Latest/Hotfixes/>

<ftp://ftp.rockliffe.com/MailSite/Latest/Hotfixes/>

For 6.x series apply the following patch:

<ftp://ftp.rockliffe.com/MailSite/6.1.22/Hotfixes/>

<ftp://ftp.rockliffe.com/MailSite/6.1.22/Hotfixes/>

Disclosure Timeline:

01/06/2006 – Issue Discovered

01/06/2006 – Reported to the vendor

01/19/2006 – Patch Released

01/20/2006 – Advisory Released

ADDITIONAL INFORMATION

The information has been provided by os2a.bto@xxxxxxxx OS2A BTO.

=====

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@xxxxxxxxxxxxxxxx

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

=====
=====

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: [*\[UNIX\] Fetchmail Bouncing Message DoS*](#)
- Next by Date: [*\[EXPL\] Cisco Aironet Wireless Access Points DoS \(ARP, Exploit\)*](#)
- Previous by thread: [*\[UNIX\] Fetchmail Bouncing Message DoS*](#)
- Next by thread: [*\[EXPL\] Cisco Aironet Wireless Access Points DoS \(ARP, Exploit\)*](#)
- Index(es):
 - ◆ [*Date*](#)
 - ◆ [*Thread*](#)