

[NEWS] @Mail Web Interface Multiple Security Vulnerabilities

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-12/0032.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 12/09/03

To: list@securiteam.com

Date: 9 Dec 2003 16:19:37 +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>

@Mail Web Interface Multiple Security Vulnerabilities

SUMMARY

<<http://www.atmail.com>> @Mail "is a feature rich Email solution that allows users to access email-resources via the web or a variety of wireless devices. The software incorporates a complete email-server package to manage and host user email at your domain(s)".

Multiple security vulnerabilities has been found in the @Mail web interface which could allow a remote attacker in the worst case to gain access to user's mailbox.

DETAILS

@Mail allows two different types of installation:

a) Flat file install

All profiles and messages of the @Mail users stored in files. This storage method is recommended for user bases < 10,000 users.

b) SQL database install (MySQL)

User profiles and messages are stored in a SQL database.

Securiteam: [NEWS] @Mail Web Interface Multiple Security Vulnerabilities

Vulnerability 1: Flat file install – Input Validation Error

'showmail.pl' fails to validate 'Folder' request parameter which allows an attacker to point it to mailbox of any registered user in @Mail system.

Vulnerability 2: SQL database install – Multiple SQL Injection

Vulnerabilities

Multiple SQL Injection vulnerabilities have been found in @Mail web interface. User supplied input is not filtered before being used in a SQL query. Consequently, query modifications are possible. Successful exploitation could allow a remote attacker to read any email messages for any email address registered in @Mail system.

Affected scripts – 'atmail.pl', 'search.pl', 'reademail.pl'.

Vulnerability 3: SQL database install – Session Hijacking Vulnerability

When user is logs into @Mail through web interface his session id and mailbox name are saved in a cookie. Modification of mailbox name allows a attacker to gain access to victim's mailbox. Victim's session ID must be active for this attack to be successful.

Vulnerability 4: Both types of installation – Cross Site Scripting

Vulnerability in 'showmail.pl'

By injecting specially crafted JavaScript code in URL and tricking a user to visit it a remote attacker can steal session id and gain access to victim's mailbox.

Proof of concept:

Vulnerability 1

Platforms: @Mail 3.52 Demo for Windows NT/2000/XP on Windows 2000 Advanced Server

The following url will give access to victim@somehost.com's mailbox

<http://www.site.com/showmail.pl?Folder=../../victim@somehost.com/mbox/Inbox>

Vulnerability 2

Platforms: @Mail 3.52 Demo for Windows NT/2000/XP on Windows 2000 Advanced Server

Through SQL Injection vulnerability in 'search.pl' an attacker can find message id for any message of any registered user. The following URL open message with message id '666' for user 'victim@atmail.com'

http://www.site.com/reademail.pl?id=666&folder=qwer'%20or%20EmailDatabase_v.Account='victim@atmail.com&t

Vulnerability 3

Platforms: @Mail 3.52 Demo for Windows NT/2000/XP on Windows 2000 Advanced Server

1. Attacker logs into @Mail web interface.
2. Attacker changes mailbox name in a cookie to victim's mailbox name:

Securiteam: [NEWS] @Mail Web Interface Multiple Security Vulnerabilities

Account&hacker%40somehost.com&SessionID&1064305709fzvpjackee =>
Account&victim%40somehost.com&SessionID&1064305709fzvpjackee

3. Attacker opens web interface of victim's email box by visiting the following URL

<http://www.site.com/parse.pl?file=html/english/xp/xplogin.html>.

Vulnerability 4

Platforms: @Mail 3.52 Demo for Windows NT/2000/XP on Windows 2000 Advanced Server

[http://www.site.com/showmail.pl?Folder=<script>alert\(document.cookie\)</script>](http://www.site.com/showmail.pl?Folder=<script>alert(document.cookie)</script>)

Vendor status:

S-Quadra alerted @Mail's development team to these issues on 02 Dec 2003. No response has been received. No fix available.

ADDITIONAL INFORMATION

The original advisory is available at:

<<http://www.s-quadra.com/advisories/Adv-20031209.txt>>
<http://www.s-quadra.com/advisories/Adv-20031209.txt>.

The information has been provided by <mailto:cipher@s-quadra.com> Nick Gudov of S-Quadra.

=====

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.