

[NT] Buffer Overflow Vulnerability found in MailMax

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-04/0029.html>

From: support@securiteam.com

Date: 04/18/03

From: support@securiteam.com

To: list@securiteam.com

Date: 18 Apr 2003 11:54:53 +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

In the US?

Contact Beyond Security at our new California office housewarming rates on automated network vulnerability scanning. We also welcome ISPs and other resellers!

Please contact us at: 323-882-8286 or ussales@beyondsecurity.com

Buffer Overflow Vulnerability found in MailMax

SUMMARY

MailMax is a "scalable e-mail server that supports SMTP, IMAP4, and POP3 protocols. Its TCP/IP GUI allows server administration from any Internet connected server. The Web Admin module allows you to define domain administrators so they can maintain their own accounts. It also provides anti-spamming options."

There is a problem in the program allowing an attacker to cause a buffer overflow in the IMAP4 protocol, within the IMAP4rev1 SmartMax IMAPMax 5, causing the service to execute arbitrary code.

DETAILS

Vulnerable systems:

* IMAP4rev1 SmartMax IMAPMax 5 (5.0.10.6 and 5.0.10.7)

Immune systems:

* IMAP4rev1 SmartMax IMAPMax 5 (5.0.10.8)

Securiteam: [NT] Buffer Overflow Vulnerability found in MailMax

* IMAP4rev1 SmartMax IMAPMax 5.5

The vulnerability is a buffer overflow in the IMAP4rev1 SmartMax IMAPMax 5. The overflow occurs whenever a malicious attacker sends a large amount of characters within the password field.

The following transcript demonstrates a sample exploitation of the vulnerabilities:

```
----- [Transcript] -----  
nc 127.0.0.1 143  
* OK IMAP4rev1 SmartMax IMAPMax 5 Ready  
0000 CAPABILITY  
* CAPABILITY IMAP4rev1  
0000 OK CAPABILITY completed  
0001 LOGIN "mail@mail.com" "A..[50] ..A"  
0001 NO Invalid user name or password.  
0001 NO Invalid user name or password.
```

```
----- [Transcript] -----
```

When this attack is used there will pop-up a message box on the server, with the text "Buffer overrun detected! – Program: <PATH>\IMAPMax.exe" at this time the service shuts down (a long enough buffer will overwrite the EIP allowing execution of arbitrary code), and has to be restarted manually, from the service manager.

Workarounds:

* With this vulnerable version of IMAP, the only workaround is to disable the IMAP4rev1 SmartMax IMAPMax 5 service, there are no workaround in the configuration.

* SmartMax has released a patched version of IMAPMax.exe version 5.0.10.8 which corrects the problem. It can be downloaded at <ftp://ftp.smartmax.com/updates/MailMax 5.0/Files/> Remember to ensure that the file version is 5.0.10.8 or higher.

* Update your MailMax Version 5 to the released version 5.5

Vendor response:

"Thank you for the buffer overrun security notification in our ImapMax module for MailMax 5. I'm enclosing an updated IMAPMAX which fixes the buffer overflow vulnerability? We'll be posting this in our MailMax 5.5 update next week.

Regards,
Eric Weber"

Disclosure timeline:

25/03/2003 Found the Vulnerability, and made an analysis.

27/03/2003 Reported to Vendor (sales@smartmax.com, features@smartmax.com, support@smartmax.com).

Securiteam: [NT] Buffer Overflow Vulnerability found in MailMax

27/03/2003 Vendor reply, they now know of the vulnerabilities.
27/03/2003 Vendor send a patch (Version 5.0.10.7) of the IMAPMax.exe still contains the vulnerability.
27/03/2003 Received version 5.0.10.8 from Vendor.
27/03/2003 Tested version 5.0.10.8 from vendor, and this version is not vulnerable.
27/03/2003 Fix made public.
11/04/2003 Public Disclosure.

ADDITIONAL INFORMATION

The vulnerability was discovered and reported by
<<mailto:der@infowarfare.dk>> Dennis Rand.

=====

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.