

[NEWS] Clearswift MAILsweeper MIME Attachment Evasion Issue

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-03/0020.html>

From: support@securiteam.com

Date: 03/09/03

From: support@securiteam.com

To: list@securiteam.com

Date: 9 Mar 2003 15:41:27 +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

Clearswift MAILsweeper MIME Attachment Evasion Issue

SUMMARY

<<http://www.mimesweeper.com/products/msw/default.asp>> MIMESweeper is a family of products designed to implement email and web communications e-policies. MIMESweeper delivers the capabilities for organizations to protect themselves against email and web based threats, meet legal and regulatory requirements, implement productivity saving policies and manage the intellectual property passing through their network.

A vulnerability in the product allows attackers to use a technique that would allow them to pass through MAILsweeper undetected. This is done by using malformed MIME encapsulation techniques.

DETAILS

Vulnerable systems:

* Clearswift MAILsweeper version 4.x

Securiteam: [NEWS] Clearswift MAILsweeper MIME Attachment Evasion Issue

```
////wAAAAAAAAFQBAAAAAIAUkKL6IzABRAADh+jBAADB
gwAjsCLDgYAi/lPi/f986RQuDQAUMuMw4zYSI7YjsC/Dw
C5EACw//OuR4v3i8NIjsC/DwCxBIvG99DT6IzaK9BzBIz
YK9LT4APwjtqLx/fQ0+iMwivQcwSMwCvS0+AD+I7CrIrQ
Tq2LyEaKwiT+PLB1BazzqusGPLJ1bfOkisKoAXSxvjIBD
h+LHgQA/DPSrYvI4xOLwgPDjsCti/iD//90ESYBHeLzgf
oA8HQWgcIAEOvcjMBAjsCD7xAmAR1IjsDr4ovDiz4IAIs
2CgAD8AEGAgAtEACO2I7AuWAA+o7Wi+f7i8Uu/y+0QLsC
ALkWAizKjtq6HAHNIbj/TM0hUGFja2VkJGZpbGUGaXMgY
29ycnVwdAEAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAA=
```

Step 3: To reproduce this issue, send an email containing the attachment created in step 2 that will be processed by the scenario from step 1. This should result in a successful discovery condition.

Step 4: Reopen the attachment from step 2 and remove the first line (MIME-Version: 1.0), then resend the attachment as per step 3. This should result in the attachment not being spotted as an executable.

Recommendations:

To be an effective tool, the MAILsweeper product must not only be able to process encoding techniques implemented as per the relevant standard, but also common misinterpretations.

As an ongoing process, a study project should be undertaken by Clearswift to identify applications that routinely decode MIME objects and have a liberal interpretation of the MIME standard.

In response to this advisory, Clearswift have produced an updated script utility that can detect the malformed MIME header used in this example [3]. This should be implemented until a more permanent solution is forthcoming.

ADDITIONAL INFORMATION

References:

[1] <<http://www.clearswift.com>> <http://www.clearswift.com>

[2] <<http://www.rfc.net/rfc2045.html#s4>>
<http://www.rfc.net/rfc2045.html#s4>

[3] <<http://www.clearswift.com/support/threatlab/vbstool.asp>>
<http://www.clearswift.com/support/threatlab/vbstool.asp>

The information has been provided by <<mailto:bugtraq@corsaire.com>> Martin O'Neal.

=====

Securiteam: [NEWS] Clearswift MAILsweeper MIME Attachment Evasion Issue

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.