

[NEWS] Clearswift MAILsweeper Multiple Encoding/Compression Issues

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-08/0049.html>

From: SecuriTeam (*support_at_securiteam.com*)

Date: 08/15/04

To: list@securiteam.com

Date: 15 Aug 2004 14:07:13 +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>

Clearswift MAILsweeper Multiple Encoding/Compression Issues

SUMMARY

The MAILsweeper product provides policy based, email content security functionality. Part of this functionality allows the product to block attachments based on the type of content (i.e. executable) or name of the attachment.

Encoding and compression technology is now commonly used to make the transfer of data by email more efficient. Due to this, it is essential that a product such as MAILsweeper can detect and analyze the content contained within, or at least "fail closed" if a positive identification cannot be made.

However, MAILsweeper does not detect a number of common compression formats (for which it is listed as compatible) and in certain circumstances also fails to identify the name of file attachments when they are encoded.

DETAILS

Vulnerable Systems:

Securiteam: [NEWS] Clearswift MAILsweeper Multiple Encoding/Compression Issues

* Clearswift MAILsweeper version 4.3.14 and prior

Immune Systems:

* Clearswift MAILsweeper version 4.3.15 or newer

Analysis:

The MAILsweeper attachment detection functionality works by recursively analyzing the email message body for container constructs (such as MIME and compressed archives etc.), decoding these and then comparing the contents against a predefined policy.

The current product

<<http://www.clearswift.com/products/msw/smtp/techspec.asp>> spec sheet lists that the product is compatible with "ARJ (including self-extracting ARJ), GZip, RAR, TAR, PGP, LZH, LHA, CMP, ZIP (multiple variants), BinHex and CAB, MIME, UUE, TNEF, and binary". This is a subset of the available compression formats, but does cover the majority of those in common use.

For analysis purposes, a collection of the freely available compression tools was assembled. A sample executable file was then added to each container type and then these were passed through a MAILsweeper host configured with the latest available patches (CS MAILsweeper 4.3 for SMTP Hotfix 4.3.10 and Technology Update 1.4.10).

The results were as per the following table. Where version information for the archive tool was available, it is listed:

Encoding Listed Detected Content Detected filenames

7ZIP (2.30)	No	No	No
ACE (2.2)	No	No	No
ARC (6.0)	No	No	No
ARJ (2.81)	Yes	Yes	Yes
BH	No	No	No
BASE64	No	Yes	n/a
Binary	Yes	Yes	n/a
BINHEX	Yes	Yes	No
BZIP2 (1.0.2)	No	No	No
CAB	Yes	Yes	Yes
CMP	Yes	Not tested	Not tested
COMPRESS (4.2.4) ...	No	Yes	Yes
GZIP (1.2.4)	Yes	Yes	Yes
HAP (3.05)	No	No	No
HPK (.78a0)	No	No	No
IMG	No	No	No
JAR	No	Yes	Yes
LHA (2.55e)	Yes	Yes	Yes
LZH (1.13c)	Yes	Yes	Yes
MIME	Yes	Yes	Yes
PAK (2.51)	No	No	No
PGP	Yes	Yes	Yes
RAR (2.90)	Yes	Yes	Yes

Securiteam: [NEWS] Clearswift MAILsweeper Multiple Encoding/Compression Issues

RAR (3.20) Yes No No
RAWRITE (0.7) No No No
DOS TAR (1.12) Yes As Undetermined ... As Undetermined
UNIX TAR (1.13) Yes As Undetermined ... As Undetermined
TNEF Yes Yes Yes
UUE Yes Yes n/a
ZIP (2.04g) Yes Yes Yes
ZIP (6.0d) Yes As Undetermined ... As Undetermined
ZOO (2.1) No No No

Note: The CMP compression format was not analyzed as the tool appears to be available on the Mac only and a suitable platform was not on hand during testing.

In summary:

- There are a significant number of common formats that are not detected by MAILsweeper (most notably the newer formats like 7ZIP and ACE).
- The TAR format that is listed as compatible doesn't seem to be supported, producing a "corrupt" error for all versions tested.
- Several formats that are listed as compatible are actually version dependent (RAR and ZIP).
- The BinHex (HGX) format is detected but it does not expose the filenames contained within to scrutiny.

The MAILsweeper product works from a starting position of allowing all content to pass, then specifically blocking undesirable attachments. By virtue of the encoding formats not being detected, the container and the contents are passed through the system without being analyzed.

Recommendations:

Clearswift have released the 4.3.15 Hotfix that corrects these issues. This should be applied to all existing installations where appropriate.

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0928>>
CAN-2003-0928,
<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0929>>
CAN-2003-0929 and
<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0930>>
CAN-2003-0930.

History:

Discovered: 07.08.03
Vendor notified verbally: 26.08.03
Vendor notified in writing: 05.11.03
Vendor patch released: 05.08.04
Document released: 13.08.04

As per the normal process for dealing with Clearswift, after months of requesting a status update on these issues (without any response), the

Securiteam: [NEWS] Clearswift MAILsweeper Multiple Encoding/Compression Issues

patches for these vulnerabilities have been released without any discussion or coordination with ourselves, and as is becoming the norm, completely un-attributed.

ADDITIONAL INFORMATION

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

The original article can be found at:

<<http://www.corsaire.com/advisories/c030807-001.txt>>

<http://www.corsaire.com/advisories/c030807-001.txt>

=====

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.