

[Full-Disclosure] Corsaire Security Advisory – Clearswift MAILsweeper multiple encoding/compression issues

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2004-08/0663.html>

From: advisories (advisories_at_corsaire.com)

Date: 08/13/04

To: <full-disclosure@lists.netsys.com>

Date: Fri, 13 Aug 2004 17:42:14 +0100

— Corsaire Security Advisory —

Title: Clearswift MAILsweeper multiple encoding/compression issues

Date: 07.08.03

Application: Clearswift MAILsweeper prior to 4.3.15

Environment: Windows 2000

Author: Martin O'Neal [martin.oneal@corsaire.com]

Audience: General distribution

Reference: c030807-001

— Scope —

The aim of this document is to clearly define a MIME attachment evasion issue in the MAILsweeper product, as supplied by Clearswift Ltd. [1]

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

— Overview —

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 analyse 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.

-- Analysis --

The MAILsweeper attachment detection functionality works by recursively analysing 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 spec sheet [2] 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
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 analysed 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 (HQX) 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 analysed.

— Recommendations —

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

— CVE —

The Common Vulnerabilities and Exposures (CVE) project has assigned Multiple numbers to this issue:

CAN-2003-0928 Clearswift MAILsweeper RAR 3.20 container detection issue
CAN-2003-0929 Clearswift MAILsweeper ZIP 6.0 container detection issue
CAN-2003-0930 Clearswift MAILsweeper HQX container filename detection issue

These are candidates for inclusion in the CVE list, which standardises names for security problems (<http://cve.mitre.org>).

-- References --

- [1] <http://www.clearswift.com>
- [2] <http://www.clearswift.com/products/msw/smtp/techspec.asp>

-- Revision --

- a. Initial release.
- b. Added CVE reference.
- c. Revised to include vendor patch.

-- Distribution --

This security advisory may be freely distributed, provided that it remains unaltered and in its original form.

-- Disclaimer --

The information contained within this advisory is supplied "as-is" with no warranties or guarantees of fitness of use or otherwise. Corsaire accepts no responsibility for any damage caused by the use or misuse of this information.

-- About Corsaire --

Corsaire are a leading information security consultancy, founded in 1997 in Guildford, Surrey, UK. Corsaire bring innovation, integrity and analytical rigour to every job, which means fast and dramatic security performance improvements. Our services centre on the delivery of information security planning, assessment, implementation, management and vulnerability research.

A free guide to selecting a security assessment supplier is available at <http://www.penetration-testing.com>

Copyright 2003 Corsaire Limited. All rights reserved.

Full-Disclosure – We believe in it.
Charter: <http://lists.netsys.com/full-disclosure-charter.html>