

[VulnWatch] Corsaire Security Advisory – Multiple vendor MIME separator issue

Source: <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2004-09/0010.html>

From: advisories (advisories_at_corsaire.com)

Date: 09/13/04

To: <advisories@corsaire.com>

Date: Mon, 13 Sep 2004 12:47:05 +0100

— Corsaire Security Advisory —

Title: Multiple vendor MIME separator issue

Date: 04.08.03

Application: various

Environment: various

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

Audience: General distribution

Reference: c030804-006

— Scope —

The aim of this document is to clearly define a MIME content evasion issue that affects a variety of products including; browsers, proxy servers, email clients, content security gateways and antivirus products.

— History —

Discovered: 04.08.03 (Martin O'Neal)

NISCC notified: 28.01.04

Document released: 13.09.04

— Overview —

There are a number of content security gateway and antivirus products available that provide policy based security functionality. Part of this functionality allows the products to block embedded file attachments based on their specific content type, such as executables or those containing viruses. However, by using malformed MIME encapsulation techniques centred on the presence of non-standard separators, this functionality can be evaded.

— Analysis —

The MIME standards are intended to provide a common mechanism to exchange data between systems and are used extensively by protocols such as HTTP and SMTP. The structure of a MIME message is defined in RFC2045 [1], which in turn makes use of concepts introduced in RFC822 [2] (superseded by RFC2822 [3]).

The standards define a range of fields that control how data is encoded within the transport, and how it should be interpreted by the receiving agent. For example, RFC2822 states "Header fields are lines composed of a field name, followed by a colon (":"), followed by a field body, and terminated by CRLF". No advice is given for situations in which the colon separator (or any of the other separators used within the MIME standard) is used incorrectly, such as when it is doubled or omitted entirely.

As usual, this lack of clarity within an RFC has been interpreted in various ways by the assorted vendors. For many products, such as email clients and browsers, this scope for interpretation might only result in some unreliable behaviour. However, for a collection of security products, being unaware of the various ways that the standard has been interpreted can lead to more serious results, as the products may fail to detect a threat within the data stream.

When a receiving agent is presented with a MIME message that contains unexpected or missing separators, it tends to respond in one of three broad ways:

- It identifies the MIME message as malformed and blocks it.
- It fails to interpret the MIME field (or message).
- It correctly interprets the MIME field (or message).

The first of the three would be the correct behaviour for a security conscious product, but based on empirical research this is not the common result for a number of scenarios.

The MIME field separator issue has been observed to affect most of the headers, parameters and values defined within the standard. To use this issue as an attack mechanism, all that is required is to identify a target that has a client agent that interprets the chosen separator more liberally than any security products that protect it.

— Recommendations —

To be effective tools, the security products must not only be able to process encoding techniques implemented as per the relevant standard, but also common misinterpretations and deliberate corruptions.

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

VulnWatch: [VulnWatch] Corsaire Security Advisory – Multiple vendor MIME separator issue

NISCC have produced a document consolidating a number of vendor statements on these issues [4]. Contact your vendor directly to establish whether you are affected by these issues.

-- Background --

This issue was discovered using a custom SMTP/HTTP vulnerability analysis tool developed by Corsaire's security assessment team. This tool is not available publicly, but is an example of the specialist approach used by Corsaire's consultants as part of a commercial security assessment. To find out more about the cutting edge services provided by Corsaire simply visit our web site at <http://www.corsaire.com>

-- CVE --

The Common Vulnerabilities and Exposures (CVE) project has assigned the name CAN-2004-0052 to this issue. This is a candidate for inclusion in the CVE list (<http://cve.mitre.org>), which standardises names for security problems.

-- References --

- [1] <http://www.faqs.org/rfcs/rfc2045.html>
- [2] <http://www.faqs.org/rfcs/rfc822.html>
- [3] <http://www.faqs.org/rfcs/rfc2822.html>
- [4] <http://www.uniras.gov.uk/vuls/2004/380375/mime.htm>

-- Revision --

- a. Initial release.
- b. Released.

-- 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

VulnWatch: [VulnWatch] Corsaire Security Advisory – Multiple vendor MIME separator issue 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.