Internet Engineering Task Force (IETF)
Request for Comments: 6692
Updates: 6591
Category: Standards Track
ISSN: 2070-1721

R. Clayton
University of Cambridge
M. Kucherawy
Cloudmark, Inc.

July 2012

Source Ports in Abuse Reporting Format (ARF) Reports

Abstract

This document defines an additional header field for use in Abuse Reporting Format (ARF) reports to permit the identification of the source port of the connection involved in an abuse incident.

This document updates RFC 6591.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc6692.

Table of Contents

1. Introduction

[ARF] defined the Abuse Reporting Format, an extensible message format for Email Feedback Reports. These reports are used to report incidents of email abuse. ARF was extended by [AUTHFAILURE-REPORT] to enable the reporting of email authentication failures. These specifications provided for the source IP address to be included in a report. As explained in [LOG], the deployment of IP address sharing techniques requires the source port values to be included in reports if unambiguous identification of the origin of abuse is to be achieved.

This document defines an ARF reporting field to contain this information and provides guidance for its use.

2. Keywords

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [KEYWORDS].

3. Source-Port Field Definition

A new ARF header field called "Source-Port" is defined. When present in a report, it MUST contain the client port of the TCP connection from which the reported message originated, corresponding to the "Source-IP" field that contains the client address of that same connection, thereby describing completely the origin of the abuse incident.

Per, [ABNF], the formal syntax is:

```
source-port = "Source-Port:" [CFWS] 1*5DIGIT [CFWS] CRLF
```

"CFWS", which represents email-style comments or folding white space, is imported from [MAIL].

When any report is generated that includes the "Source-IP" field (see Section 3.2 of [ARF]), this field SHOULD also be present, unless the port number is unavailable.

Use of this field is RECOMMENDED for reports generated per [AUTHFAILURE-REPORT] (see Section 3.1 of that document).

4. Time Accuracy

[LOG] underscores the importance of accurate clocks when generating reports that include source port information because of the fact that source ports can be recycled very quickly in Internet Service Provider environments. The same considerations described there apply here.

Report generators that include an Arrival-Date report field MAY choose to express the value of that date in Universal Coordinated Time (UTC) to enable simpler correlation with local records at sites that are following the provisions of [LOG].

5. IANA Considerations

IANA has added the following entry to the "Feedback Report Header Fields" registry:

Field Name: Source-Port

Description: TCP source port from which the original message was received

Multiple Appearances: No

Related "Feedback-Type": any

Reference: [RFC6692]

Status: current

6. Security Considerations

This extension introduces no new security considerations not already covered in [ARF].

Some security considerations related to the general topic of source port logging can be found in [LOG].

7. References

7.1. Normative References

[ABNF] Crocker, D. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", STD 68, RFC 5234, January 2008.

[ARF] Shafranovich, Y., Levine, J., and M. Kucherawy, "An Extensible Format for Email Feedback Reports", RFC 5965, August 2010.

[AUTHFAILURE-REPORT] Fontana, H., "Authentication Failure Reporting Using the Abuse Reporting Format", RFC 6591, April 2012.

[KEYWORDS] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[MAIL] Resnick, P., Ed., "Internet Message Format", RFC 5322, October 2008.

7.2. Informative References

[LOG] Durand, A., Gashinsky, I., Lee, D., and S. Sheppard, "Logging Recommendations for Internet-Facing Servers", BCP 162, RFC 6302, June 2011.

Appendix A. Acknowledgements

The authors wish to acknowledge the following for their review and constructive criticism of this proposal: Steve Atkins, Scott Kitterman, John Levine, and Doug Otis.

The idea for this work originated within the Messaging Anti-Abuse Working Group (MAAWG).

Authors' Addresses

Richard Clayton
University of Cambridge
Computer Laboratory
JJ Thomson Avenue
Cambridge CB3 0FD
United Kingdom

Phone: +44 1223 763570
EMail: richard.clayton@cl.cam.ac.uk

Murray S. Kucherawy
Cloudmark, Inc.
128 King St., 2nd Floor
San Francisco, CA 94107
US

Phone: +1 415 946 3800
EMail: superuser@gmail.com