TCP Maintenance and Minor Extensions (tcpm)
Internet-Draft
Updates: 793 (if approved)
Intended status: Standards Track
Expires: September 30, 2012

F. Gont
UTN-FRH / SI6 Networks

March 29, 2012

Processing of TCP segments with Mirrored End-points
draft-gont-tcpm-tcp-mirrored-endpoints-00.txt

Abstract

This document describes a problem found in some popular implementations regarding the processing of TCP segments in which the local endpoint is equal to the remote endpoint. Additionally, it formally updates RFC 793 clarifying how this scenario should be handled.

Status of this Memo

Copyright Notice

Table of Contents

1. Introduction

Some systems have been found to be unable to process TCP segments in which the source endpoint {Source Address, Source Port} is the same than the destination end-point {Destination Address, Destination Port}. Such TCP segments have been reported to cause malfunction of a number of implementations [CERT1996], and have been exploited in the past to perform Denial of Service (DoS) attacks [Meltman1997]. While these packets are very very unlikely to exist in legitimate scenarios, TCP should nevertheless be able to process them without the need of any "extra" code.

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 RFC 2119 [RFC2119].

2. Updating RFC 793

TCP MUST be able to gracefully handle the case where the source end-point (IP Source Address, TCP Source Port) is the same as the destination end-point (IP Destination Address, TCP Destination Port).

> A SYN segment in which the source end-point {Source Address, Source Port} is the same as the destination end-point {Destination Address, Destination Port} will result in a "simultaneous open" scenario, such as the one described in page 32 of RFC 793 [RFC0793]. Therefore, those TCP implementations that correctly handle simultaneous opens should already be prepared to handle these unusual TCP segments.

3. IANA Considerations

This document has no IANA actions. The RFC Editor is requested to remove this section before publishing this document as an RFC.

4. Security Considerations

This document describes a problem found in some popular implementations regarding the processing of TCP instances in which the local and the remote TCP endpoints are the equal. It formally updates RFC 793, clarifying how such packets should be handled, thus helping prevent unexpected behaviors in host implementations.

5. Acknowledgements

The author would like to thank David Borman for a fruitful discussion about this topic at IETF 73 (Minneapolis).

This document is based on the technical report "Security Assessment of the Transmission Control Protocol (TCP)" [CPNI-TCP] written by Fernando Gont on behalf of the UK CPNI.

Fernando Gont would like to thank the UK CPNI for their continued support.

6. References

6.1. Normative References

[RFC0793] Postel, J., "Transmission Control Protocol", STD 7, RFC 793, September 1981.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

6.2. Informative References

[CERT1996]
CERT, "CERT Advisory CA-1996-21: TCP SYN Flooding and IP Spoofing Attacks", 1996, <http://www.cert.org/advisories/CA-1996-21.html>.

[CPNI-TCP]
Gont, F., "CPNI Technical Note 3/2009: Security Assessment of the Transmission Control Protocol (TCP)", 2009, <http://www.gont.com.ar/papers/tn-03-09-security-assessment-TCP.pdf>.

[Meltman1997]
Meltman, "new TCP/IP bug in win95. Post to the bugtraq mailing-list", 1996, <http://insecure.org/sploits/land.ip.DOS.html>.

Author's Address

Fernando Gont
UTN-FRH / SI6 Networks
Evaristo Carriego 2644
Haedo, Provincia de Buenos Aires 1706
Argentina

Phone: +54 11 4650 8472
Email: fgont@si6networks.com
URI: http://www.si6networks.com