TCP Maintenance and Minor Extensions
Internet-Draft
Intended status: Informational
Expires: February 12, 2017

L. Velvindron
hackers.mu

August 11, 2016

Handling of TCP ACK throttling
draft-lvelvindron-ack-throttling-02

Abstract

The functionality provided by the TCP ACK throttling mechanism can be exploited as a side channel vulnerablity to terminate connections between two arbitrary hosts and inject data in the communication stream.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on February 12, 2017.

Table of Contents

1. Introduction

[RFC5961] defines the challenge ACK response mechanism as a technique to mitigate against blind in-window attacks. Specifically, an ACK packet is sent in response to an incoming segment with a SYN bit to confirm that the preceding connection was lost. Another case is sending an ACK packet if the RST packet is received but the sequence number does not match the next expected sequence number. Lastly, to prevent data injection, the range of valid ACK value is reduced for better strictness, so the likelihood of old ACK values and very new ACK values are discarded. In all of those cases, the ACK packet is referrered to as a "Challenge ACK" through the rest of this document.

[RFC5961] also introduces an ACK throttling mechanism to reduce possible wastage of CPU and bandwidth resources by limiting the number of challenge ACK that can be sent in a given interval.

An attacker can leverage the Challenge ACK and the ACK throttling mechanism to abuse on the global ACK throttling rate-limit on a target host. Through a series of step, the attacker can send spoofed packets to the target host, affect the the global challenge ACK rate-limiter, count the number of challenge ACK received, and finally compare that number with the target system limit.

The attacker can then gather clues about: the existence of a 4-tuple connection, the next expected sequence number, and the expected ACK number.

Based on the gathered information, the attacker can mount connection reset attacks and data injection attacks. Those attacks have been demonstrated to work in real-world constraints according to [CBR01].

Due to the seriousness of the threat, it is sufficient to deprecate the ACK throttling mechanism, as defined in [RFC5961].

This document updates [RFC5961].

1.1. Terminology

Challenge ACK in this document denotes the ACK packet sent in response to an segment whose RST bit is set and the sequence number does not fully match the next expected sequence value, but is within the current receive window as defined in [RFC5961].

The keywords MUST, MUST NOT, REQUIRED, SHALL, SHALL NOT, SHOULD, SHOULD NOT, RECOMMENDED, MAY, and OPTIONAL, when they appear in this document, are to be interpreted as described in [RFC2119].

2. Deprecation of ACK throttling mechanism

An implementation is not required to implement an ACK throttling mechanism which is conservative as defined in section 7 of [RFC5961]. However, if there is a concern about CPU or bandwidth usage, an implementation may have a per-socket ACK throttling mechanism which is not shared across the system. This makes it more difficult to abuse compared to having a single (global) ACK throttling mechanism. Additionally, an implementation may also introduce a randomized value to the interval defined in Section 7 of [RFC5961]. This makes the attacks defined in section 1 much more difficult.

3. Operations

It will take time to update all of the TCP implementations that fully implement the ACK throttling mechanism as described in [RFC5961].

An operator can increase the value of the ACK throttling limit to the highest value possible to mitigate the risk of the vulnerabilities defined in section 1.

4. IANA Considerations

None of the proposed measures have an impact on IANA.

5. Security Considerations

The purpose of this document is to deprecate a feature of TCP that has been shown to lead to security vulnerabilities. Specific examples of those vulnerabilities can be found in [CBR01]. In particular, the ACK throttling mechanism leads to a side-channel vulnerability that can be leveraged for connection reset and data injection attacks. A description of this functionality can be found in section 1.

6. Normative References

[CBR01] Cao, Y., Wang, Z., Dao, T., Krishnamurthy, S., and L. Marvel, "Off-Path TCP Exploits: Global Rate Limit Considered Dangerous", University of California , 2016.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

[RFC5961] Ramaiah, A., Stewart, R., and M. Dalal, "Improving TCP's Robustness to Blind In-Window Attacks", RFC 5961, DOI 10.17487/RFC5961, August 2010, <http://www.rfc-editor.org/info/rfc5961>.

Author's Address

Loganaden Velvindron
hackers.mu
88 Avenue De Plevitz Roches Brunes
Rose Hill 71259

Phone: +230 59762817
Email: logan@hackers.mu