ASA BEAST Vulnerability Solutions

Document ID: 118854

Contributed by Atri Basu, Loren Kolnes, and Narendra Meka, Cisco
TAC Engineers.
Apr 01, 2015

Contents

Introduction

This document describes a vulnerability within the Cisco Adaptive Security Appliance (ASA) sowftware that allows unauthorized users to access protected content. Workarounds for this issue are also described.

Problem

The Browser Exploit Against SSL/TLS (BEAST) vulnerability is leveraged by an attacker in order to effectively read protected content via Initialization Vector (IV) chaining in Cipher Block Chaining (CBC) encryption mode with a known plaintext attack.

The attack uses a tool that exploits a vulnerability in the widely−used Transport Layer Security Version 1 (TLSv1) protocol. The issue is not rooted in the protocol itself, but rather the cipher suites that it uses. The TLSv1 and Secure Sockets Layer Version 3 (SSLv3) favor CBC ciphers, where the Padding Oracle attack occurs.

User Impact

As indicated by the SSL Pulse SSL implementation survey, created by the Trustworthy Internet Movement, over 75% of SSL servers are susceptible to this vulnerability. However, the logistics involved with the BEAST tool are fairly complicated. In order to use BEAST to eavesdrop on traffic, an attacker must have the ability to read and inject packets very quickly. This potentially limits the effective targets for a BEAST attack. For example, a BEAST attacker can effectively grab random traffic at a WIFI hot spot or where all Internet traffic is bottlenecked through a limited number of network gateways.

Solution

BEAST is an exploit of the weakness in the cipher that is used by the protocol. Since it affects the CBC cipher, the original workaround for this issue was to switch to the RC4 cipher instead. However, the Weaknesses in the Key Scheduling Algorithm of RC4 article that was published in 2013 reveals that even RC4 had a weakness that made it unsuitable.

In order to workaround this issue, Cisco has implemented these two fixes for the ASA:

- Cisco bug ID CSCts83720: *Upgrade to TLS 1.1/1.2*

Upgrade and use TLS 1.1/1.2. The limitation with this solution is that it applies only to ASA 5500−X ASA Platforms. The encryption hardware on legacy ASA platforms (ASA 5505 and the ASA 5500 series) do not support TLSv1.2. As a result, a fix for these platforms is not feasible.

Due to protocol limitations, there is no solution for SSLv3 or TLSv1.0; however, most modern browsers have implemented different ways of mitigation.

- Cisco bug ID CSCuc85781: *WebVPN Cookie Randomization*

  For the ASA software versions that do not support TLSv1.2, Cisco made the cookies random with this fix in order to reduce the risk. This does not completely prevent BEAST attacks, but it helps mitigate them.

Tip: The only way to be completely protected from the BEAST vulnerability is to use TLSv1.2. This is similar to ciphers. Cisco continues to add newer, stronger ciphers in newer code, and older ciphers might have known issues (such as RC4). Thus, Cisco recommends that you move to the newer protocols and ciphers.

Updated: Apr 01, 2015 Document ID: 118854