SSL/TLS Information Disclosure (BEAST) Vulnerability

Overview

This article discusses the exposure of SecureAuth IdP Appliances to the BEAST vulnerability as described in CVE-2011-3389.

Applies to

SecureAuth IdP Version	OS Version
7.x+	• Windows Server 2008 • Windows Server 2008 R2 • Windows Server 2012 • Windows Server 2012 R2

Discussion

What is BEAST?

Short for **B**rowser **E**xploit **A**gainst **S**SL/**T**LS, BEAST is a browser exploit against SSL/TLS that was revealed in late September 2011. This attack leverages weaknesses in cipher block chaining (CBC) to exploit the Secure Sockets Layer (SSL) / Transport Layer Security (TLS) protocol. The CBC vulnerability can enable man-in-the-middle (MITM) attacks against SSL in order to silently decrypt and obtain authentication tokens, thereby providing hackers access to data passed between a Web server and the Web browser accessing the server.

Are SecureAuth IdP Appliances impacted?

SecureAuth IdP Appliances use the Microsoft Windows Server operating system which is impacted by the BEAST vulnerability. The vulnerability affects the protocol itself and is not specific to the Windows operating system or SecureAuth IdP. See the Mitigation section below for ways to address this vulnerability.

Mitigation

Operating System Mitigation

Ensure the SecureAuth IdP Appliance is fully patched with the latest Microsoft Windows Server updates.

Web Browser Mitigation

Ensure end-users are running a modern and fully patched Web browser that includes protection against the BEAST attack. Major browser vendors have added workarounds to mitigate the attack since BEAST is primarily an attack against Web browsers.

TLS 1.0 Disablement

Disable TLS 1.0 and have users connect using TLS 1.1 or TLS 1.2 protocols which are immune to the BEAST attack. TLS 1.0 is now considered insecure and disabling the protocol improves the overall security of the SecureAuth IdP Appliance.

Before disabling the TLS 1.0 protocol, SecureAuth recommends auditing the network for legacy devices that require the protocol for operation. If there is a device reliant upon the TLS 1.0 protocol and it is disabled, that device will no longer be able to communicate with the Appliance. To disable the protocol, SecureAuth recommends using the SecureAuth Crypto Tool which automates the process.

SecureAuth IdP Appliances ship with SSL 3.0 disabled as the protocol is now considered insecure. If this protocol is currently enabled for compatibility with legacy applications, it must be disabled along with TLS 1.0 to fully mitigate the BEAST attack.

As with procedures recommended for TLS 1.0, an audit of the network should be conducted before disabling the SSL 3.0 protocol.

When the BEAST vulnerability was first discovered it was commonly suggested that administrators emphasize RC4 ciphers over CBC to mitigate the vulnerability. However, in the intervening years, multiple issues have been discovered with RC4 which makes it a larger security risk than BEAST. SecureAuth advises against using RC4 ciphers to mitigate BEAST at this time.