THREAT BRIEF

Gartner
COOL VENDOR 2020™

CurveBall (CVE-2020-0601)

Exposing Elliptic Curve Cryptography-Based Certificate Spoofing
Winter 2020

Details of a vulnerability in Windows operating systems known as CurveBall were revealed as part of Microsoft's January 2020 Patch Tuesday release. The heart of the vulnerability allows adversaries to create fraudulent Certificate Authority (CA) certificates, which are the top portion of the pyramid of digital-certificate trust. Properly validated CAs ensure that corporations such as Microsoft can cryptographically trust certificates in the downstream chain. This mechanism is fundamental to digital-certificate trust infrastructure. CurveBall enables capable attackers to introduce "spoofed" certificates into that chain, undermining trusted web browsing and potentially exposing people to malware or privacy breaches.

The underlying vulnerability in CurveBall deals with a malfunctioning Dynamic Link Library by the name of Crypt32. Specifically, Crypt32 fails to parse key parameters within an Elliptic Curve Cryptography-based (ECC) certificate. Crypt32 processes only the public key of a CA certificate, allowing complete control over a cryptographic function, known as the Generator or Base. When attackers control this value, they can associate a known public key with a completely new and controlled private key of their choosing. With a spoofed CurveBall CA in hand, they can exploit two very impactful attack vectors:

1. Signing malware to appear trusted by a legitimate entity, such as Microsoft
2. Creating fraudulent SSL certificates that can be used to decrypt secure web traffic

Trusted and signed binaries are often a critical part of endpoint protection, and cryptographically trusted and verified SSL certificates underpin the foundation of secure web browsing. As a result, hackers with exploits for these attack vectors can severely disrupt networks with unpatched Windows 10, Server 2016, and Server 2019 machines.

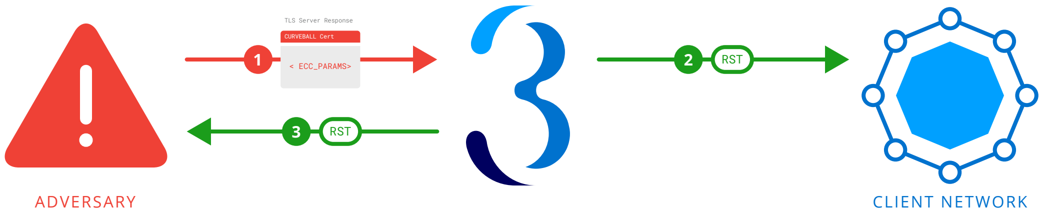
Neutralizing the Use of Fraudulent Certificates

Trinity Cyber detects both of CurveBall's attack vectors within a network session. Our detection methodology focuses on examining the generic properties of ECC certificates within both signed binaries and the actual protocol of Transport Layer Security (TLS) enabled web sessions. Using this approach, we avoid the pitfalls of traditional indicator-based IDS/IPS solutions, while maximizing the accuracy in detecting CurveBall attacks.

When we detect ECC certificates within either attack vector, we take the following actions in real time to prevent it:

1. Remove CurveBall-signed binaries from a network session while allowing the session to continue and;
2. Gracefully close TLS sessions that contain CurveBall SSL certificates.

These unique actions minimize risk and maintain critical business operations for our clients by effectively neutralizing Curveball attacks in real time.



sales@trinitycyber.com • (240) 842-9900 • trinitycyber.com

Trinity Cyber was named a Cool Vendor in Gartner's Cool Vendors in Network and Endpoint Security, Mark Harris, Rob Smith, et al., 30 September 2020.

The GARTNER COOL VENDOR badge is a trademark and service mark of Gartner, Inc., and/or its affiliates, and is used herein with permission. All rights reserved. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's Research & Advisory organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

Trinity Cyber