telelink
BUSINESS SERVICES

Advanced Security Operations Center
Telelink Business Services
www.telelink.com

Chain of Fools/ Curveball attack (CVE-2020-0601)

Emerging Threat Bulletin
Prepared: 17.01.2020

Chain of fools/ Curveball attack

Executive summary

Digital certificates have long been used by the computing and security industries to place a seal of authenticity and trust in both local content and network communications. Vulnerabilities in the mechanisms designed to validate these certificates can undermine this trust relationship and provide avenues that attackers can exploit and eventually use to compromise computer systems.

Reported privately by a United States government entity to Microsoft, the Windows CryptoAPI Spoofing Vulnerability (CVE-2020-0601) is an important vulnerability that affects certificate validation in Windows 10, Windows Server 2016, and Windows Server 2019. An attacker can exploit this vulnerability by crafting certificates that appear to have been signed by legitimate providers.

This vulnerability is due to a certificate validation error in the *crypt32.dll* library in Windows that allows spoofing of certificates derived from trusted Elliptic Curve Cryptography (ECC) root certificates. Because of errors in the validation mechanism, malicious files and hijacked TLS connections can appear to have trusted ECC root certificates, including root certificates signed by Microsoft.

While our security researchers have not seen active exploitation of this vulnerability at the time of publication, we are providing applicable protection coverage for customers. In addition to the fixes that address CVE-2020-0601 in the January 2020 security updates (released January 14, 2020), Microsoft has released various behavioral and indicator-based detections designed to identify and block exploitation attempts.

Possible attack scenarios

This vulnerability can make attacks involving the following techniques possible:

- Man-in-the-middle attacks against TLS connections made through web browsers, such as Microsoft Edge, Internet Explorer, or Chrome
- Man-in-the-middle attacks against channel-based TLS connections over various protocols or services, such as LDAP, IIS, RPC, EAP-TLS, WFP, or TERMSRV
- Use of forged certificates that add legitimacy to phishing and watering hole websites
- Delivery and execution of malicious files disguised under forged signing certificates
- Installation of malicious App Compat shims that could enable code injection in system processes

The following attack scenarios demonstrate how attacks that deliver malicious files or hijack secure communications might unfold.

Signature verification of files

An attacker can sign malware with a spoofed certificate that appears to have been derived from a trusted root certificate. The malware is then able to bypass various security controls depending on the certificate verification used by the security control and the identity of the root signer.

Malware signed with a spoofed certificate that is derived from a Microsoft ECC root certificate will run with the trust level given to Microsoft binaries in Windows. On vulnerable endpoints, signed malware can possibly bypass AppLocker and Windows Defender Application Control. However, Windows Defender Antivirus remains unaffected as it doesn't scan for ECC certificates during certificate verification.

Certificate chain validation

An attacker can imitate either a server or a client during TLS communication. To perform this attack, the attacker abuses the same public key and generates a forged signature. Afterwards, the attacker can use the forged certificate to spoof or intercept TLS authentication.

By using forged certificate chains, the attacker can increase the chances of a successful man-in-the-middle attack. The same technique might also be used during DNS hijacking, phishing, or watering hole attacks.

An attacker, for example, might set up a phishing website to contain a forged certificate. Web browsers that visit this website is then unable to correctly determine that the website isn't truly owned by the certificate signer and display appropriate warnings. Consequently, the visiting user interacts with the phishing site believing that it is trustworthy.

Likewise, an attacker can imitate a website visitor using a forged certificate. The website itself is unable to validate the identity of the visitor causing it to grant access to resources that are otherwise only accessible to the legitimate holder of that certificate.

More sophisticated attackers that perform man-in-the-middle attacks and other network interception techniques can leverage forged certificates to feign legitimacy. Instead of redirecting TLS authentication packets prior to manipulating traffic, they can use the forged certificate to directly establish a trusted connection with either the client or the server and begin to manipulate traffic from there. Communications involving vulnerable endpoints are therefore more susceptible to man-in-the-middle attacks.

Unaffected components

Certificate verification mechanisms used by the following Windows components are *not* affected by attacks that exploit this vulnerability:

- Windows kernel-mode code integrity validation, which uses *minCrypt*
- Windows Update, which uses a dual-certificate chain validation involving both RSA and ECC
- Xbox and Xbox Live, which use an unaffected form of ECC that doesn't rely on ECDSA certificates
- Azure real-time operating system (RTOS), which also doesn't rely on ECDSA certificates
- Windows Hello
- Windows Defender Antivirus, which doesn't scan for ECC certificates

Mitigations

- Apply the January 2020 security updates to address CVE-2020-0601. This security update ensures that Windows CryptoAPI completely validates ECC certificates.
- On endpoints running Windows 10, Windows Server 2016, and Windows Server 2019, disallow third-party root certificates when possible and explicitly pin your root certificates to your internal domains.

References

- Windows CryptoAPI Spoofing Vulnerability. Microsoft (accessed 2020-01-14)
- January 2020 security updates. Microsoft (accessed 2020-01-14)
- CVE-2020-0601. Mitre (accessed 2020-01-14)
- National Security Agency Cybersecurity Advisory
- Original Blog post
- Proof of Concept
- Microsoft Threat Intelligence