CrowdStrike Delivers Protection for Critical Windows Certificate Spoofing Vulnerability

January 24, 2020 Hamilton Yang and Scott Taschler Endpoint Protection

Microsoft recently disclosed a critical vulnerability (CVE-2020-0601) that could be leveraged for a wide range of malicious actions including spoofing trusted websites or software.

The word “critical” is used regularly to describe vulnerabilities, but it’s very rare for the U.S. National Security Agency (NSA) to weigh in directly as they did on this vulnerability. In addition to Microsoft’s release, the NSA released a cybersecurity advisory recommending immediate patching. This advisory, combined with the fact that proof-of-concept (POC) exploits have been released publicly, means that this vulnerability must be taken seriously, and it requires quick action.

CrowdStrike® gives its customers a set of powerful capabilities, including some specifically tailored to this emerging threat, to help keep them safe and to provide the visibility necessary to manage the associated risks.

About CVE-2020-0601

This Windows vulnerability could allow an attacker to craft TLS (transport layer security) certificates that appear to originate from a trusted certificate authority (CA). Such a certificate could be used for a wide variety of malicious purposes, including intercepting and manipulating HTTPS traffic, or delivering malicious executables that appear to be signed by the OS vendor. It affects Windows 10, as well as Windows Server 2016 and 2019.

As of the publication date of this blog, no malicious exploits of this vulnerability have been observed being used by attackers "in the wild," but POC code has been released by multiple security researchers. Working POC code increases the likelihood of malicious usage of this vulnerability in the near future, and most researchers agree that it's only a matter of time before attackers begin leveraging this vulnerability in real-world attacks. All authorities on the subject, including Microsoft and the NSA, recommend immediate patching of this critical vulnerability.

How CrowdStrike Protects Customers

A number of controls are now available in the CrowdStrike Falcon® platform to provide customers with protection from threats and visibility into security postures across their organizations.

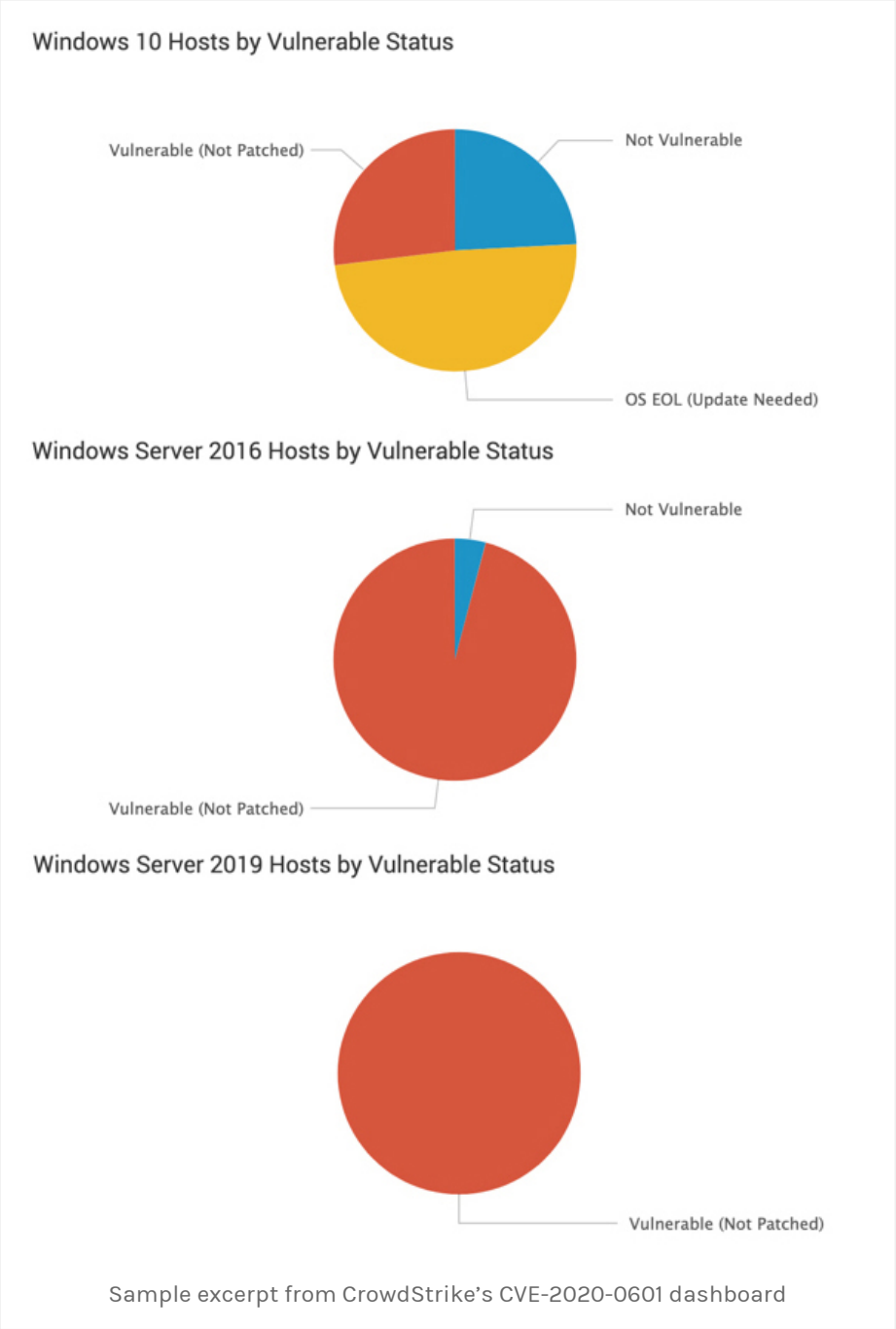
- Falcon continues to provide the highest levels of malware defense, mitigating the risks associated with spoofed code-signing certificates. Spoofed code-signing certificates allow an attacker to make it appear that their malicious software originates from a trusted source, such as a large, known software developer, bypassing trust-based code execution controls.

  Falcon's lightweight agent uses kernel-level APIs for validating executable signatures, which are not vulnerable to CVE-2020-

0601. As a result, Falcon properly disregards signatures that are spoofed using this vulnerability, ensuring that administrators don't miss a threat because it appears to have a valid signature.

In addition, Falcon leverages multiple detection layers, including cloud-scale machine learning combined with behavioral techniques, which make it highly effective at detecting and blocking malicious code, regardless of the trust level the local OS may associate with it.

- CrowdStrike has also created a dashboard to identify systems vulnerable to CVE-2020-0601. The dashboard is provided free of charge to customers who have the CrowdStrike endpoint detection and response (EDR) solution, Falcon Insight™.



Sample excerpt from CrowdStrike's CVE-2020-0601 dashboard

CrowdStrike customers can use this dashboard to get a high-level view of their exposure to CVE-2020-0601, updated continuously in real time without additional scanning or overhead.

CrowdStrike customers can access this new dashboard by navigating to **Investigate > Event Search > Vulnerability Dashboards > CVE-2020-0601 (Windows CryptoAPI Spoofing)**.

Customers using Falcon Spotlight™, CrowdStrike's vulnerability management module, can leverage it to obtain more extensive visibility, including comprehensive reports showing current exposure and trends related to CVE-2020-0601.

- CrowdStrike has released an updated build of the lightweight Falcon agent (v5.23). This agent update includes new telemetry events that indicate attempts to actively exploit the vulnerability on a patched Windows system. These events provide customers with early warning of in-the-wild attacks targeting CVE-2020-0601, and can be used to help prioritize patching and investigations.

  Customers can keep a watchful eye for these events, described in the release notes for Windows Sensor 5.23 (available in the Falcon UI under **Support > News**), to monitor for exploit attempts within their environments. Any relevant events are conveniently incorporated into the above CVE-2020-0601 dashboard for immediate visibility.

Together, these security controls provide excellent protection, as well as the visibility needed to understand exposure and hunt for active threats. To see these security controls in action, watch the CVE-2020-0601 Defense Demonstration video we have created specifically for this threat.

Additional Resources:

- *Watch the Falcon platform CVE-2020-0601 defense demo.*
- *Read the Microsoft Security Vulnerability announcement.*
- *Read the NSA Cybersecurity Advisory.*
- *Learn more about CrowdStrike vulnerability management by visiting the Falcon Spotlight webpage.*
- *Find out more about the CrowdStrike Falcon platform by visiting the webpage.*
- *Test CrowdStrike next-gen AV for yourself. Start your free trial of Falcon Prevent™ today.*