

Date: January 16, 2020
From: ADP Global Security Organization
Subject: Microsoft CryptoAPI Spoofing Vulnerability – CVE-2020-0601

ADP has recently learned of the Microsoft CryptoAPI Spoofing Vulnerability – CVE-2020-0601 that could allow an attacker to exploit the vulnerability by using a spoofed code-signing certificate to sign a malicious executable, making it appear the file was from a trusted, legitimate source. Affected systems include Microsoft Windows 10, Server 2016, and Server 2019, some Server Core installations (V1803 | V1903 | V1909).

At this time, ADP has determined that none of its internal systems have been compromised by this attack, and no intrusion has occurred. ADP's layered defense includes technologies and controls to identify and/or prevent these types of threats, including assessing vulnerabilities and applying appropriate protection and detection control updates.

ADP's Global Security Organization continues to actively monitor this situation as it does with all reported vulnerabilities. Clients are encouraged to visit ADP's website at www.adp.com/trust to learn more about how ADP protects data, and how clients can help protect themselves.

Protecting our clients and their data from malicious activity is a top priority for ADP.