When Microsoft released patches on January 14, 2020, it revealed one of the most critical vulnerabilities it has discovered in years. The company confirmed a serious security vulnerability in the way Windows CryptoAPI (Crypt.dll) validates Elliptic Curve Cryptography (ECC) certificates, disclosed to the company by the NSA. Given the severity of the vulnerability, Microsoft and the wider security community were unanimous in their immediate call to install the relevant patch - the only available mitigation at this time.

The vulnerability affects Windows 10 and Windows Server 2016/2019 as well as applications that rely on Windows for authentication and other types of trust functionality. Regular internet users will recognize cryptographic certificates as the security mechanisms that keep them safe when browsing secure websites, such as banking websites. They can be recognized in internet browsers when browsing HTTPS URLs, usually witnessed with a padlock icon near the web address. As the DHS directive states:

It bypasses the trust store, allowing unwanted or malicious software to masquerade as authentically signed by a trusted or trustworthy organization, which may deceive users or thwart malware detection methods like anti-virus.

Additionally, a maliciously crafted certificate could be issued for a hostname that did not authorize it, and a browser that relies on Windows’ CryptoAPI would not issue a warning, allowing an attacker to decrypt, modify, or inject data on user connections without detection.

CVE-2020-0601
Critical Windows CryptoAPI Spoofing Vulnerability

Patch Patch Patch

Given the severity of the vulnerability, it is highly recommended to review patching schedules to ensure that Microsoft’s most recent patches are installed as soon as possible.

On 14 January, Microsoft claimed that there were no known attacks which had exploited CVE-2020-0601. However, with the vulnerability in the open, doubtless various threat actors will swiftly be building tools to exploit it, if they have not done so already. The NSA has already stated that “sophisticated cyber actors will understand the underlying flaw very quickly.”

In a statement, a Microsoft Senior Director confirmed that those that are applying automatic updates should already be protected. In the event that enterprise-wide, automated patching is not possible, the NSA has recommended system owners prioritize patching endpoints that provide essential or broadly relied-upon services.
In their advisory on the vulnerability, the NSA described the consequences of not patching as “severe and widespread.” Anne Neuberger, Head of the NSA’s Cyber Security Directorate, recommended that network owners, “expedite implementation of the patch immediately, as we will also be doing.” At the time of writing, Microsoft and other cyber security providers claimed their updated software was able to detect and respond to malicious activity designed to exploit the vulnerability.

**Why so serious**

As news of the vulnerability broke over the past week, some news sources reported that Microsoft had already provided a patch to the US military and various critical service providers who are bound by non-disclosure agreements, indicating the severity of the issue. The Department of Homeland Security also issued an emergency directive to patch all affected endpoints within 10 days, and strongly recommended patching immediately.

As discussed earlier, if exploited, the vulnerability allows attackers to spoof cryptographic certificates, undermining the chain of trust between systems, which is the foundation of many key security functions on the local network and the internet.

As more information becomes available, we will look to Microsoft for a deeper technical analysis of this issue. However, if network systems can’t reliably verify the identity of other systems they are communicating with, what software they should install or who it’s written by, then it leaves security gaps for attackers to take control. With Windows 10 installed on over 900 million devices, the urgency of the response is understandable.

1 Source: [https://www.wired.com/story/nsa-windows-10-vulnerability-disclosure/](https://www.wired.com/story/nsa-windows-10-vulnerability-disclosure/)