THE WINDOWS CURVEBALL VULNERABILITY AND WHAT YOU CAN DO ABOUT IT

What is Curveball?

I like to watch baseball, and am amazed at pitchers who can throw a good curveball. However, due to the unnatural motion required to throw it, the curveball is a more advanced pitch and can injure a pitcher's elbow and shoulder. Now there's a new type of curveball to be concerned about, but instead of hurting a pitcher, this one can hurt your network.

"Curveball" is a new security vulnerability in the Windows operating system and it needs to be remediated quickly, the clock is ticking and time is running out. It is known as CVE-2020-0601 (Common Vulnerability Exposure) and is also known as "Chain of Fools." The U.S. The National Vulnerability Database gives it a CVSS (Common Vulnerability Scoring System) rating of 8.1 on a scale of 1-10, placing it near WannaCry (8.5) and Docker Doomsday (8.6).

The Curveball vulnerability affects Windows Server 2016, Windows Server 2019, and Windows 10. It exists in the Windows crypt32.dll, which is a cryptographic module in Windows that implements certificate and cryptographic messaging functions in Microsoft's CryptoAPI. It validates software application certificates and checks the signatures of transport layer security (TLS) certificates to ensure they are safe. These certificates begin with a trusted root certificate authority (CA). Certificates that start with a trusted root CA can sign other certificates, which then sign other certificates, etc. This forms a "chain of trust" where all the certificates in the chain point back to the

trusted root CA.

Why is Curveball Dangerous?

Exploitation of this vulnerability allows malicious code to be delivered that appears to be from a trusted source. An attacker can trick crypt32 into thinking a certificate was signed by a trusted root authority when in fact it was not. This enables attacks that include:

1. Delivery of false website certificates that look legitimate, and cause a user to fall victim to a phishing attack.
2. Man-in-the-Middle attacks, where the attacker can decrypt traffic moving between a user's system and the internet and obtain sensitive information,
3. Malware can be signed to appear legitimate, and fool the OS into thinking it can be trusted,

What should you do about Curveball?

The answer to this vulnerability is a Microsoft security patch (available now), and it needs to be deployed quickly. Word on the street is that attempts to exploit the vulnerability have already begun. The NSA (credited with discovering Curveball and informing Microsoft) has rated it as "severe" and is saying that sophisticated hackers can understand the weakness quickly and exploit it. They further advise that all January 2020 Patch Tuesday patches be installed as quickly as possible on Windows 10 and Windows Server 2016/2019 systems.

How should it be Remediated?

Last year an average of 1,500 vulnerabilities per month were reported in the National Vulnerability Database (NVD) and this is likely to continue. Manual remediation methods can no longer keep up with the quantity and sophistication of vulnerabilities, and automated solutions have become a requirement. Not only is speed needed, but your automation solution should have the following:

- Integration with leading vulnerability scanners and the ability to ingest scanner data,
- Advanced analytics and intelligence to transform vulnerability data into actionable information. Your solution needs to quickly analyze vulnerability data, determine severities, identify business services exposed, and help set priorities,
- Automated mapping of vulnerabilities, patches, and configuration changes to the servers and networking devices affected, and acquisition of the remediation (i.e. patch) required
- State-of-the-art, ease-of-use features including simplified patching, automation consoles specially designed for patching, dashboards with drill-down capabilities, visibility to vulnerabilities on unmapped assets, and the ability to reduce the amount of vulnerability "noise" operations teams deal with. This usually consists of removing vulnerabilities that have already been remediated, or are about to be, from scanner data.
- Vulnerability remediation planning, scheduling, and execution where the process is performed in accordance with disciplined change management.
- The vulnerability remediation process should further be augmented with Discovery solutions for blind spot detection and mapping of potential attack paths that could be taken by an intruder (lateral movement).

New choices for deployment models also are available. Organizations can now choose between

hybrid solutions with components located both in the cloud and on-premises, or traditional on-premises installations. Both offer advantages, but the benefits of hybrid cloud solutions based on a SaaS model are very compelling and the industry is quickly heading in that direction. I recommend taking a close look at BMC's hybrid cloud solutions for automated vulnerability management because they can quickly and easily remediate the Curveball vulnerability.

Check out the web pages for the Vulnerability Management Maturity Model to help determine where your organization is positioned and next steps, and BMC Helix Remediate and BMC Helix Vulnerability Management to learn more about how BMC can help you address serious threats including Curveball before time runs out.