CYBERSECURITY ADVISORY

Critical Vulnerabilities in Microsoft Windows Operating Systems

Last Revised: January 14, 2020 **Alert Code:** AA20-014A

Summary

New vulnerabilities are continually emerging, but the best defense against attackers exploiting patched vulnerabilities is simple: keep software up to date. Timely patching is one of the most efficient and cost-effective steps an organization can take to minimize its exposure to cybersecurity threats.

On January 14, 2020, Microsoft released software fixes to address 49 vulnerabilities as part of their monthly Patch Tuesday announcement. Among the vulnerabilities patched were critical weaknesses in Windows CryptoAPI, Windows Remote Desktop Gateway (RD

Gateway), and Windows Remote Desktop Client. An attacker could remotely exploit these vulnerabilities to decrypt, modify, or inject data on user connections:

- **CryptoAPI spoofing vulnerability – CVE-2020-0601:** This vulnerability affects all machines running 32- or 64-bit Windows 10 operating systems, including Windows Server versions 2016 and 2019. This vulnerability allows Elliptic Curve Cryptography (ECC) certificate validation to bypass the trust store, enabling unwanted or malicious software to masquerade as authentically signed by a trusted or trustworthy organization. This could deceive users or thwart malware detection methods such as antivirus. 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.
- **Windows RD Gateway and Windows Remote Desktop Client vulnerabilities – CVE-2020-0609, CVE-2020-0610, and CVE-2020-0611:** These vulnerabilities affect Windows Server 2012 and newer. In addition, CVE-2020-0611 affects Windows 7 and newer. These vulnerabilities—in the Windows Remote Desktop Client and RD Gateway Server—allow for remote code execution, where arbitrary code could be run freely. The server vulnerabilities do not require authentication or user interaction and can be exploited by a specially crafted request. The client vulnerability can be exploited by convincing a user to connect to a malicious server.

The Cybersecurity and Infrastructure Security Agency (CISA) is unaware of active exploitation of these vulnerabilities. However, because patches have been publicly released, the underlying vulnerabilities can be reverse-engineered to create exploits that target unpatched systems.

CISA strongly recommends organizations install these critical patches as soon as possible—prioritize patching by starting with mission critical systems, internet-facing systems, and networked servers. Organizations should then prioritize patching other affected information technology/operational technology (IT/OT) assets.

Technical Details

CryptoAPI Spoofing Vulnerability – CVE-2020-0601

A spoofing vulnerability exists in the way Windows CryptoAPI (Crypt32.dll) validates ECC certificates.

According to Microsoft, “an attacker could 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. The user would have no way of knowing the file was malicious, because the digital signature would appear to be from a trusted provider.” Additionally, “a successful exploit could also allow the attacker to conduct man-in-the-middle attacks and decrypt confidential information on user connections to the affected software.”[1] <https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/cve-2020-0601>

A cyber attacker could exploit CVE-2020-0601 to obtain sensitive information, such as financial information, or run malware on a targeted system; for example:

- **A maliciously crafted certificate could appear to be issued for a hostname that did not authorize it,** preventing a browser that relies on Windows CryptoAPI from validating its authenticity and issuing warnings. If the certificate impersonates a user’s bank website, their financial information could be exposed.
- **Signed malware can bypass protections (e.g., antivirus) that only run applications with valid signatures.** Malicious files, emails, and executables can appear legitimate to unpatched users.

The Microsoft Security Advisory for CVE-2020-0601 <https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/cve-2020-0601> addresses this vulnerability by ensuring that Windows CryptoAPI completely validates ECC certificates.

Detection Measures

The National Security Agency (NSA) provides detection measures for CVE-2020-0601 in their Cybersecurity Advisory: Patch Critical Cryptographic Vulnerability in Microsoft Windows Clients and Servers <https://media.defense.gov/2020/jan/14/2002234275/-1/-1/0/csa-windows-10-crypt-lib-20190114.pdf>.[2] <https://media.defense.gov/2020/jan/14/2002234275/-1/-1/0/csa-windows-10-crypt-lib-20190114.pdf>

Windows RD Gateway Vulnerabilities – CVE-2020-0609/CVE-2020-0610

According to Microsoft, "A remote code execution vulnerability exists in Windows Remote Desktop Gateway (RD Gateway) when an unauthenticated attacker connects to the target system using RDP and sends specially crafted requests. This vulnerability is pre-authentication and requires no user interaction."[3] <https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/cve-2020-0609>,[4] <https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/cve-2020-0610>

CVE-2020-0609/CVE-2020-0610:

- Affects all supported Windows Server versions (Server 2012 and newer; support for Server 2008 ends January 14, 2020);
- Occurs pre-authentication; and
- Requires no user interaction to perform.

The Microsoft Security Advisories for CVE-2020-0609 <https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/cve-2020-0609> and CVE-2020-0610 <https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/cve-2020-0610> address these vulnerabilities.

Windows Remote Desktop Client Vulnerability – CVE-2020-0611

According to Microsoft, “A remote code execution vulnerability exists in the Windows Remote Desktop Client when a user connects to a malicious server. An attacker who successfully exploited this vulnerability could execute arbitrary code on the computer of the connecting client.”[5] <https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/cve-2020-0611>

CVE-2020-0611 requires the user to connect to a malicious server via social engineering, Domain Name Server (DNS) poisoning, a man-in the-middle attack, or by the attacker compromising a legitimate server.

The Microsoft Security Advisory for CVE-2020-0611 <https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/cve-2020-0611> addresses this vulnerability.

Impact

A successful network intrusion can have severe impacts, particularly if the compromise becomes public and sensitive information is exposed. Possible impacts include:

- Temporary or permanent loss of sensitive or proprietary information,
- Disruption to regular operations,
- Financial losses relating to restoring systems and files, and
- Potential harm to an organization’s reputation.

Mitigations

CISA strongly recommends organizations read the Microsoft January 2020 Release Notes page <https://portal.msrc.microsoft.com/en-us/security-guidance> for more information and apply critical patches as soon as possible—prioritize patching by starting with mission critical systems, internet-facing systems, and networked servers. Organizations should then prioritize patching other affected IT/OT assets.

General Guidance

- Review Guide to Enterprise Patch Management Technologies, NIST Special Publication 800-40 Revision 3 <https://csrc.nist.gov/publications/detail/sp/800-40/rev-3/final>. Patch management is the process for identifying, acquiring, installing, and verifying patches for products and systems. This publication is designed to assist organizations in understanding the basics of enterprise patch management technologies. It explains the importance of patch management and examines the challenges inherent in performing patch management. It provides an overview of enterprise patch management technologies, and also briefly discusses metrics for measuring the technologies' effectiveness.
- Review CISA Insights publications <https://www.cisa.gov/insights>. Informed by U.S. cyber intelligence and real-world events, each CISA Insight provides background information on particular cyber threats and the vulnerabilities they exploit, as well as a ready-made set of mitigation activities that non-federal partners can implement. Printable materials can be found by visiting: https://www.cisa.gov/publication/cisa-insights-publications <https://www.cisa.gov/publication/cisa-insights-publications>.
- Review CISA's Cyber Essentials <https://www.cisa.gov/cyber-essentials>. CISA's Cyber Essentials is a guide for leaders of small businesses as well as leaders of small and local government agencies to develop an actionable understanding of where to start implementing organizational cybersecurity practices. Essentials are the starting point to cyber readiness. To download the guide, visit: https://www.cisa.gov/publication/cisa-cyber-essentials <https://www.cisa.gov/publication/cisa-cyber-essentials>.

References

[1] Microsoft Security Advisory for CVE-2020-0601 <https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/cve-2020-0601>

[2] NSA Cybersecurity Advisory: Patch Critical Cryptographic Vulnerability in Microsoft Windows Clients and Servers <https://media.defense.gov/2020/jan/14/2002234275/-1/-1/0/csa-windows-10-crypt-lib-20190114.pdf>

[3] Microsoft Security Advisory for CVE-2020-0609 <https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/cve-2020-0609>

[4] Microsoft Security Advisory for CVE-2020-0610 <https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/cve-2020-0610>

[5] Microsoft Security Advisory for CVE-2020-0611 <https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/cve-2020-0611>

[6] CISA Blog: Windows Vulnerabilities that Require Immediate Attention <https://www.cisa.gov/blog/2020/01/14/windows-vulnerabilities-require-immediate-attention>

[7] CERT/CC Vulnerability Note VU#849224 <https://kb.cert.org/vuls/id/849224/>

[8] CERT/CC Vulnerability Note VU#491944 <https://kb.cert.org/vuls/id/491944/>

Revisions

January 14, 2020: Initial version|January 14, 2020: Minor technical edits