Cybersecurity Threat Advisory: Microsoft Windows critical remote code execution vulnerability

blog.barracuda.com/2022/06/01/cybersecurity-threat-advisory-microsoft-windows-critical-remote-code-execution-vulnerability

June 1, 2022

Microsoft released an emergency update for a critical remote code execution vulnerability for all Windows versions that are still receiving security updates (Windows 7+ and Server 2008+). This vulnerability allows an attacker to utilize the software to execute arbitrary code from a calling application such as Word. Barracuda MSP recommends reading the instructions on the Microsoft website here or in our references section to disable the MSDT URL protocol.

What is the threat?

A remote code execution vulnerability exists in the current Windows versions 7+ and Server 2008+. An attacker who successfully executes this remote code can gain control of the Microsoft Word application. This remote code execution vulnerability exists when the Microsoft Support Diagnostic Tool (MSDT) is called using the URL protocol from Word. This vulnerability has been categorized as a zero-day, indicating that it was an unknown flaw.

Why is it noteworthy?

This vulnerability exists in all current Microsoft Windows versions which is the operating system that supports a computers basic function such as executing applications and controlling peripherals. Microsoft has been impacted by similar zero-day vulnerabilities dating back to 2009. With news of this zero-day vulnerability coming to light, attackers are likely to accelerate attacks on targets where possible, while that window remains open.

What is the exposure or risk?

When exploited, this vulnerability allows an attacker to have complete and unrestricted access to the Windows application. If an attacker has privileges of the calling application, they can easily install programs, view, change, delete data, or create new accounts in the context allowed by the user's rights. These privileges give the attacker the tools to conduct a ransomware event and Business Email Compromise (BEC) that can lead to temporary or permanent loss of sensitive or proprietary information, disruption to regular operations, financial losses, and potential harm to an organization's reputation.

What are the recommendations?

Barracuda recommends the following actions to limit the impact of an arbitrary code execution attack:

- Following our reference link to disable the MSDT URL protocol.
- Be observant of any new potential unauthorized activity.
- Keep all applications updated thus enforcing new security measures
- Continue to stay up to date with our threat advisories for updates.

References

For more in-depth information about the recommendations, please visit the following links:

- Guidance for CVE-2022-30190 Microsoft Support Diagnostic Tool Vulnerability – Microsoft Security Response Center
- Barracuda Solutions for Ransomware | Barracuda
- 13 Email Threat Types to Know About Right Now | Barracuda