SecurityRisk ADVISORS

Threat Bulletin

Microsoft Windows Support Diagnostic Tool Zero-Day Vulnerability

Executive Summary

On May 30th, 2022, Microsoft released a security update acknowledging the MSDT remote code execution vulnerability. The security update details the dangers of the exploit with Microsoft explaining that "an attacker who successfully exploits this vulnerability can run arbitrary code with the privileges of the calling application. [And proceed to] install programs, view, change, delete data, or create new accounts in the context allowed by the user's rights."

Affected Products

All Windows 7+ and Server 2008+ products are affected.

Safeguards/Recommendations

Microsoft recommends disabling MSDT URL protocol because it prevents troubleshooters being launched as links including links throughout the operating system. To disable the protocol run Command Prompt as Administrator and execute the command "reg export HKEY_CLASSES_ROOT \ms-msdt filename" to back up the registry. Finally, run the command "reg delete HKEY_CLASSES_ROOT\ms-msdt /f".

References

https://msrc-blog.microsoft.com/2022/05/30/guidance-for-cve-2022-30190-microsoft-support-diagnostic-tool-vulnerability/

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-30190

https://gist.github.com/matthewB-huntress/14ab9d309f25a05fc9305a8e7f351089

https://github.com/GossiTheDog/ThreatHunting/blob/master/AdvancedHuntingQueries/Follina-Office.ahq

Vendor: Microsoft

CVE-ID: CVE-2022-30190

Published: May 30, 2022

CVSS V3 Overall score: 7.8

Criticality: High

Patch Availability: No

Vulnerability Type: Remote Code Execution

Exploitability Metrics

Attack Vector: Local

Attack Complexity: Low

Privileges Required: None

User Interaction: Required

Impact Metrics

Scope: Unchanged

Confidentiality: High

Integrity: High

Availability: High

Confidence Metrics

Exploitability: Functional

Remediation Level: Temp Fix

Report Confidence: Confirmed

Version History

Version 1. Initial Report

Contact Us

24x7 SOC Phone: 215.867.9051
Email: soc@sra.io
Website: https://sra.io