AL2022_39 Microsoft patches actively exploited Follina Windows zero-day (20th June 2022)

Description

Microsoft has released security updates as part of the monthly rollup of Windows Updates to address a critical Windows zero-day vulnerability known as Follina.

Summary

This vulnerability is tracked as CVE-2022-30190. The security flaw is described as a Microsoft Windows Support Diagnostic Tool (MSDT) remote code execution bug that affects all Windows versions that are still receiving security updates (Windows 7+ and Server 2008+). When opening or previewing Word documents, Follina exploits allow threat actors to execute malicious PowerShell commands via MSDT (Arbitrary Code Execution (ACE)) attacks.

How it works

After successfully exploiting this zero-day vulnerability, an attacker can execute arbitrary code with the calling app's privileges to install programs, view, change, or delete data, and even create new Windows accounts as permitted by the compromised user's rights.

Remediation

To mitigate this threat, Microsoft strongly advises customers to install the updates to be fully protected from vulnerabilities.

The Guyana National CIRT recommends that users and administrators review this update and apply it where necessary.

References

- Gatlan, S. (2022, June 15). Microsoft patches actively exploited Follina Windows zero-day. Retrieved from BleepingComputer. https://www.bleepingcomputer.com/news/security/microsoft-patches-actively-exploited-follina-windows-zero-day/

- Security Update Guide - Microsoft Security Response Center. (2022, June 14). Retrieved from Microsoft Windows Support Diagnostic Tool (MSDT) Remote Code Execution Vulnerability. https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-30190