Computer Emergency Response Team of Mauritius
Ministry of Information Technology, Communication and Innovation

CERT-MU Security Alert

Date of Issue: 08 June 2022

CVE-2022-30190: Microsoft Support Diagnostic Tool (MSDT) Remote Code Execution Vulnerability "Follina"

Affected Systems: Microsoft Windows

Severity Level: High

Description:
A critical zero day vulnerability known as "Follina" (CVE-2022-30190) targeting Microsoft Windows systems have been identified. This vulnerability resides in the Microsoft Support Diagnostic Tool (MSDT), a tool from Microsoft that collects and sends system information back to Microsoft Support for problem diagnostics, such as issues with device drivers, hardware, etc. This tool is in all versions of Windows, including Windows Server OS. Successful exploitation of this vulnerability can allow remote and unauthenticated attackers to take control over the affected system.

This vulnerability is being exploited in the wild and now cybercriminals are using this vulnerability in phishing attacks as well as infect recipient with QBot malware. A series of initial attacks were reportedly observed in March 2022, targeting the Philippines, Nepal, and India. Now, attacks on the US and EU Government systems have been detected.

Microsoft is still working on a patch to fix this vulnerability. CERT-MU advises administrators and organisation to take quick corrective action until Microsoft releases a patch.

Corrective Action:
Administrators are advised to disable the MSDT protocol on their Windows devices after Microsoft reported active exploitation of this vulnerability in the wild.

Disabling the MSDT URL protocol prevents troubleshooters from being launched as links, including links throughout the operating system. Troubleshooters can still be accessed using the Get Help application and in System Settings as other or additional troubleshooters.

Follow these steps to disable:

1. Run Command Prompt as Administrator.
2. To back up the registry key, execute the command *"reg export HKEY_CLASSES_ROOT\ms-msdt filename"*
3. Execute the command *"reg delete HKEY_CLASSES_ROOT\ms-msdt /f".*

Report Cyber Incidents

Report cyber security incident on the **Mauritian Cybercrime Online Reporting System (MAUCORS - http://maucors.govmu.org/)**

Contact Information

Computer Emergency Response Team of Mauritius (CERT-MU)
Ministry of Information Technology, Communication and Innovation
Hotline No: (+230) 800 2378
Fax No: (+230) 208 0119
Gen. Info. : contact@cert.govmu.org
Incident: incident@cert.govmu.org
Website: http://cert-mu.govmu.org
MAUCORS: http://maucors.govmu.org