مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates-Microsoft

Tracking #:432317055

Date:09-04-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Microsoft released its monthly Patch Tuesday updates, addressing a total of 134 vulnerabilities across multiple products including a zero-day vulnerability that has been exploited in the wild by the RansomEXX ransomware group.

TECHNICAL DETAILS:

Microsoft released its monthly Patch Tuesday updates, addressing a total of 134 vulnerabilities across multiple products. This includes eleven Critical-rated remote code execution vulnerabilities and one actively exploited zero-day, **CVE-2025-29824**, affecting the Windows Common Log File System (CLFS) Driver.

The zero-day has been **exploited in the wild by the PipeMagic malware**, attributed to the **Storm-2460 threat actor**—a ransomware group that has used PipeMagic as a loader to deploy ransomware payloads. This campaign highlights the ongoing trend of **ransomware actors leveraging post-compromise EoP exploits** to escalate access and execute lateral movement, often after an initial foothold is gained via commodity malware.

Vulnerability Breakdown

The vulnerabilities patched in this update span several categories:

- **49 Elevation of Privilege Vulnerabilities**
- **9 Security Feature Bypass Vulnerabilities**
- **31 Remote Code Execution Vulnerabilities**
- **17 Information Disclosure Vulnerabilities**
- **14 Denial of Service Vulnerabilities**
- **3 Spoofing Vulnerabilities**

These figures exclude vulnerabilities in Mariner and Microsoft Edge, which were addressed earlier in the month.

Actively Exploited Zero-Day: CVE-2025-29824

- **Description**: A vulnerability in the Windows Common Log File System (CLFS) driver that allows local attackers to escalate privileges to SYSTEM.
- **Impact**: Exploited by attackers, including the RansomEXX ransomware gang, to gain full control over compromised devices.
- **Affected Systems**: Windows Server and Windows 11. Updates for Windows 10 are pending release.
- **Attack Vector**: Local

RECOMMENDATIONS:

- Prioritize Patching of CVE-2025-29824
  - Apply available patches immediately for Windows Server and Windows 11 systems.
  - Monitor for updates regarding Windows 10 availability and apply as soon as they are released.

- Update All Microsoft Products
  - Apply all available updates from the April 2025 Patch Tuesday to mitigate the 134 vulnerabilities, especially those rated Critical.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://msrc.microsoft.com/update-guide/releaseNote/2025-Apr