مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates - Microsoft

Tracking #:432316380

Date:09-10-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Microsoft released security updates to address multiple vulnerabilities in its products.

TECHNICAL DETAILS:

On October 8, 2024, Microsoft released security updates to address 121 vulnerabilities across its various products. These updates included five publicly disclosed zero-days, two of which were actively exploited. Additionally, the patch fixed three critical vulnerabilities and 114 important vulnerabilities.

Important Vulnerabilities Details:

Critical Vulnerabilities:

- **CVE-2024-43468 (CVSS 9.8)**: Microsoft Configuration Manager Remote Code Execution, allowing unauthenticated attackers to execute commands on the server.
- **CVE-2024-43582**: Vulnerability in Remote Desktop Protocol (RDP) allowing remote code execution through malicious packets.
- **CVE-2024-43488**: Visual Studio Code Arduino extension vulnerability that could bypass authentication checks for remote code execution.

Zero-Day Vulnerabilities:

- **CVE-2024-43573**: Spoofing vulnerability in Windows MSHTML platform-actively exploited in attacks
- **CVE-2024-43572**: Remote code execution vulnerability in Microsoft Management Console (MMC)-actively exploited in attacks.
- **CVE-2024-43583**: Winlogon Elevation of Privilege vulnerability, allowing SYSTEM-level access.
- **CVE-2024-6197**: Open Source Curl remote code execution vulnerability, requiring connection to a malicious server.
- **CVE-2024-20659**: Windows Hyper-V security feature bypass, allowing hypervisor and kernel compromise.

Additional Vulnerabilities in Core Components:

- **CVE-2024-43502**: Windows Kernel elevation of privilege vulnerability for highest-level access.
- **CVE-2024-43560**: Windows Storage Port Driver privilege escalation.

Microsoft Office and OpenSSH Flaws:

- **CVE-2024-43609**: Spoofing vulnerability in Microsoft Office
- **CVE-2024-43581** and **CVE-2024-43615**: Vulnerabilities in OpenSSH for Windows, allowing remote code execution.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the security updates recently released by Microsoft.

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/2024-Oct