مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Zero-Day Vulnerabilities in Microsoft Products

Tracking #:432316132

Date:08-08-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Critical zero-day vulnerabilities in Microsoft Windows operating systems that allows malicious actors to downgrade fully patched systems to a state vulnerable to previously exploited flaws.

TECHNICAL DETAILS:

A severe security threat has been identified in Microsoft Windows operating systems. Two zero-day vulnerabilities, **CVE-2024-21302** and **CVE-2024-38202**, allow malicious actors to effectively reverse security patches, rendering fully updated systems vulnerable to previously fixed exploits.

Vulnerabilities Details:

- **CVE-2024-21302- Windows Secure Kernel Mode Elevation of Privilege Vulnerability**
  - CVSS Base Score: 6.7 Medium
  - This vulnerability could allow an attacker with administrator privileges to replace current Windows system files with outdated versions, potentially reintroducing previously patched vulnerabilities and bypassing security features.
- **CVE-2024-38202 -Windows Update Stack Elevation of Privilege Vulnerability**
  - CVSS Base Score: 7.3 High
  - This vulnerability could allow an attacker with basic user privileges to "unpatch" previously fixed security vulnerabilities or bypass security features like Virtualization Based Security (VBS).

Impact

Successful exploitation of this vulnerability can lead to:

- **System compromise:** Exploitation of reintroduced vulnerabilities can grant attackers unauthorized access.
- **Data breaches:** Sensitive information protected by security features like Virtualization Based Security (VBS) could be exposed.
- **Privilege escalation:** Attackers might gain elevated privileges within the system.

Affected Systems:

- Windows systems supporting Virtualization Based Security (VBS), including specific Azure Virtual Machine SKUs (CVE-2024-21302)
- All Windows systems with backup functionality (CVE-2024-38202)

Mitigations:

While Microsoft is working on full patches, the following interim measures are strongly recommended:

For CVE-2024-21302:

- Configure audit settings to monitor file access and sensitive privilege usage.
- Regularly review Azure Active Directory risk reports for suspicious activity.

For CVE-2024-38202:

- Audit users with backup and restore permissions.
- Restrict access to backup files.
- Implement monitoring for unauthorized modifications to backup files.

RECOMMENDATIONS:

- **Prioritize Patching:** Apply official patches from Microsoft as soon as they become available.
- **Implement Strong Access Controls:** Enforce strict access controls and least privilege principles.
- **Regularly Review Security Posture:** Conduct thorough security assessments and vulnerability scans.
- **Employee Awareness:** Educate employees about the risks of social engineering and phishing attacks.

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://www.safebreach.com/blog/downgrade-attacks-using-windows-updates/
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21302
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38202