مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

High-Severity Vulnerability in Node.js 'systeminformation' Package

Tracking #:432316664
Date:24-12-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a high-severity command injection vulnerability in the widely-used Node.js systeminformation package, which could potentially be exploited to execute malicious code on affected systems.

TECHNICAL DETAILS:

Vulnerability Details:

- **CVE-2024-56334**
- **CVSS Score**: 7.8 (High)
- A command injection vulnerability exists in the getWindowsIEEE8021x function of the systeminformation package. This function retrieves network SSID information but fails to properly sanitize SSIDs before passing them to cmd.exe. Attackers can exploit this flaw by embedding malicious commands into Wi-Fi SSIDs.
- The flaw could allow attackers to execute arbitrary OS commands, potentially leading to remote code execution (RCE) or privilege escalation, depending on the context of the package's use.
- Successful exploitation of this vulnerability could lead to:
    - Remote Code Execution (RCE)
    - Privilege Escalation
    - Unauthorized System Access
    - Data Exfiltration
    - System Disruption

Affected Versions:

- All versions of **systeminformation** up to and including **5.23.6**

Fixed Versions:

- Upgrade to **systeminformation** version 5.23.7 or later

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to upgrade the affected versions to the fixed versions at the earliest.

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://nvd.nist.gov/vuln/detail/CVE-2024-56334