مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Multiple Vulnerabilities in Vonets WiFi Bridge Devices

Tracking #: 432316165
Date:20-08-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Multiple vulnerabilities in Vonets Wi-Fi Bridge Devices that could be exploited to gain unauthorized access to affected systems.

TECHNICAL DETAILS:

Multiple vulnerabilities exist in Vonets Wi-Fi Bridge Devices. Successful exploitation of these vulnerabilities could allow attackers to execute arbitrary code, disclose sensitive information, or disrupt device functionality on affected systems.

Vulnerability Details:

- **CVE-2024-39791** | CVSS v3.1 10.0 – Critical
  - The most critical vulnerability, a Stack-Based Buffer Overflow, enables attackers to execute arbitrary code remotely, potentially taking full control of the device without authentication.

- **CVE-2024-37023** | CVSS v3.1 9.1 – Critical
  - OS Command Injection vulnerabilities allow authenticated attackers to execute arbitrary operating system commands on the device, potentially giving them control over the device's operation.

- **CVE-2024-42001** | CVSS v3.1 8.6 – High
  - An Improper Authentication flaw allows attackers to bypass authentication by sending specially crafted requests when another user session is active.

- **CVE-2024-29082** | CVSS v3.1 8.6 – High
  - An Improper Access Control issue enables attackers to bypass authentication and perform a factory reset on the device via unprotected endpoints, potentially causing service disruptions and loss of configuration data.

- **CVE-2024-41936** | CVSS v3.1 7.5 – High
  - A Directory Traversal vulnerability allows attackers to read arbitrary files on the device, bypassing authentication mechanisms and exposing sensitive information.

- **CVE-2024-39815** | CVSS v3.1 7.5 – High
  - An Improper Handling of Exceptional Conditions flaw could allow attackers to cause a Denial-of-Service (DoS) condition by sending specially crafted HTTP requests to the device.

- **CVE-2024-41161** | CVSS v3.1 7.5 – High
  - A Use of Hard-coded Credentials flaw allows unauthenticated attackers to bypass authentication and gain full access to the device using pre-set administrator credentials. These credentials cannot be disabled, making this a particularly dangerous vulnerability.

Affected Products (Including but not limited to):

- VAR1200-H: Versions 3.3.23.6.9 and prior
- VAR1200-L: Versions 3.3.23.6.9 and prior
- VAR600-H: Versions 3.3.23.6.9 and prior
- VAP11AC: Versions 3.3.23.6.9 and prior
- VAP11G-500S: Versions 3.3.23.6.9 and prior
- VBG1200: Versions 3.3.23.6.9 and prior
- VAP11S-5G: Versions 3.3.23.6.9 and prior

Note: All affected products run software versions 3.3.23.6.9 and prior.

Mitigations:

- **Minimize Network Exposure**: Ensure that all control system devices and networks are not accessible from the internet. This minimizes the risk of unauthorized access.

- **Isolate Control Systems**: Place control system networks and remote devices behind firewalls and separate them from business networks to prevent cross-network attacks.

- **Secure Remote Access**: When remote access is necessary, use more secure methods such as Virtual Private Networks (VPNs). However, be aware that VPNs themselves may have vulnerabilities and should be kept up to date. The security of the VPN is also dependent on the security of the connected devices.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to apply the mitigations provided 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://www.cisa.gov/news-events/ics-advisories/icsa-24-214-08