مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Exploited Vulnerability in Array Networks AG and vxAG ArrayOS

Tracking #:432316561

Date:26-11-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability has been identified in Array Networks AG and vxAG ArrayOS and it is actively being exploited in the wild.

TECHNICAL DETAILS:

A critical vulnerability (CVE-2023-28461) has been identified in Array Networks AG and vxAG ArrayOS versions 9.4.0.481 and earlier. This improper authentication vulnerability allows unauthenticated attackers to browse the filesystem and potentially execute remote code on affected SSL VPN gateways. Given the active exploitation of this vulnerability, immediate action is required to either patch the system or upgrade to a more secure version (ArrayOS AG 10.x). Organizations must also monitor their networks for signs of exploitation and consider implementing additional safeguards like network segmentation to minimize potential damage.

- **CVE-2023-28461 (Improper Authentication)**:
  - **Vulnerability Type**: The flaw is due to improper handling of the flags attribute in HTTP headers, which leads to unauthenticated access to the system. Attackers can exploit this by sending specially crafted requests to the affected SSL VPN gateway, enabling them to execute arbitrary code or gain unauthorized access to system files.
  - **CVSS Score**:9.8 Critical
  - **Attack Vector**: This vulnerability can be exploited remotely, over the internet, without the need for authentication.
  - **Exploitability**:
    - Remote attackers can craft specific HTTP requests containing the malicious flags attribute in the header.
    - If successful, the attacker can execute arbitrary code and browse or manipulate the system's file system, significantly compromising system integrity and confidentiality.

Vulnerable Versions:

- ArrayOS AG 9.4.0.481 and earlier
- ArrayOS AG 10.x versions are not vulnerable to this issue.

Fixed Version:

- The Array AG release 9.4.0.484

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to urgently update affected systems to the latest version of ArrayOS.

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-2023-28461