Array Networks Vulnerability Exploited by Chinese Threat Actors

Overview

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has identified active exploitation of a critical vulnerability (CVE-2023-28461, CVSS 9.8) affecting Array Networks AG and vxAG secure access gateways.

Array Networks is an U.S. based networking hardware company that sells network traffic encryption tools. The company has over 5,000 customer deployments and generated $22.6M in revenue during 2024.

CVE-2023-28461, caused by missing authentication, allows attackers to execute arbitrary code remotely. An attacker could target Array AG/vxAG devices operating on vulnerable versions of ArrayOS AG 9.x to exploit this flaw.

Recently, Trend Micro revealed that the threat actor Earth Kasha (also known as MirrorFace) has been leveraging CVE-2023-28461 in attacks against compromised SSL-VPN gateways and file storage systems, specifically targeting advanced technology firms and government entities in Japan, Taiwan, and India.

Earth Kasha has been exploiting the Array vulnerability, along with weaknesses in Proself and FortiOS/FortiProxy (CVE-2023-45727 and CVE-2023-27997). After breaking in, they use tools like Cobalt Strike, LodeInfo, and NoopDoor to stay hidden and maintain access to the systems they've targeted. CISA has added CVE-2023-28461 to their Known Exploited Vulnerabilities catalog and has instructed all federal agencies to apply patches by December 16, 2024.

Aspire Protects

- **Patch –** Aspire recommends patching as soon as possible. The fix is available on the Array Support Portal.
- Mitigations for the vulnerability can be found in Array's advisory.
- Minimize internet-facing access for SSL VPN gateways.
- Apply network segmentation to protect critical systems.

TTPs to Watch

Initial Access

- Exploit Public-Facing Application (T1190) - Remote exploitation of SSL VPN vulnerabilities using crafted HTTP headers.

Persistence

- Install Web Shell (T1505.003) - Deployment of malicious scripts for ongoing access.

Command and Control

- Application Layer Protocol (T1071) - Use of common protocols for exfiltration and communication.

IoCs

There are no known IoCs associated with CVE-2023-28461 at this time. Aspire is actively monitoring and will notify customers if any are found. For more details on how we can help protect your organization, contact Aspire's Customer Success Management team.

Targeted Industries

- Advanced Technology Organizations
- Government and Public Sector

Aspire Service Offerings

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors.
  - Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyberattacks.
- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.

- Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

Supporting Documentation

Microsoft Word - Array_Networks_Security_Advisory_for_Remote_Code_Execution_Vulnerability_AG_v1.3.docx

Spot the Difference: Earth Kasha's New LODEINFO Campaign And The Correlation Analysis With The APT10 Umbrella | Trend Micro (US)

NVD - CVE-2023-28461

CISA Adds One Known Exploited Vulnerability to Catalog | CISA

Array Networks Company Profile 2024: Stock Performance & Earnings | PitchBook