مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

Active Exploitation of ArrayOS AG Command Injection Vulnerability

Tracking #:432318108

Date:09-12-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a command injection vulnerability in Array Networks ArrayOS AG (CVE-2025-66644) is being actively exploited by threat actors to deploy PHP webshells, create rogue users, and gain persistent remote access.

TECHNICAL DETAILS:

A command injection vulnerability in Array Networks ArrayOS AG (CVE-2025-66644) is being actively exploited by threat actors to deploy PHP webshells, create rogue users, and gain persistent remote access.

Vulnerability Overview

- **CVE ID:** CVE-2025-66644
- **Severity:** High (CVSS 7.2)
- **CWE:** CWE-78 – Improper Neutralization of Special Elements in OS Commands (Command Injection)
- **Affected Products:**
    - ArrayOS AG 9.4.5.8 and earlier
    - Array AG Series physical and virtual appliances
    - Systems with DesktopDirect remote access feature enabled
- **Fixed Version:** ArrayOS AG 9.4.5.9

Nature of the Vulnerability

The flaw allows authenticated attackers to execute arbitrary OS commands on vulnerable AG Series VPN appliances. Exploitation enables:

- Deployment of PHP webshells
- Creation of unauthorized administrative users
- Persistence and full system compromise
- Lateral movement inside enterprise environments

Observed Exploitation

Active exploitation since August 2025, including:

- Attack source and communication IP: 194.233.100[.]138

RECOMMENDATIONS:

- Apply Security Update-Upgrade ArrayOS to fixed version at the earliest.
- Disable DesktopDirect (If Not Required)-Disable all DesktopDirect services on AG appliances

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.cve.org/CVERecord?id=CVE-2025-66644