Array Networks Security Advisory:
Command Injection Vulnerability ID-119617

Advisory date: April 25, 2022
Updated: September 14, 2022

Overview

Command injection vulnerability ID-119617 is a web security vulnerability that allows an attacker to execute commands on AG/vxAG SSL VPN gateway. The attacker can then exploit this vulnerability to control AG/vxAG series products.

Severity: Critical

Impact

The vulnerability has NO impact on AVX, APV, ASF and AG/vxAG (running ArrayOS AG 10.x versions) series products.

For Array AG/vxAG series products running ArrayOS AG 9.x versions, attackers may exploit this vulnerability to elevate their privileges and then control the system.

Status

The following table lists the affected product and software versions. You can use this table to check whether your Array products are affected by this vulnerability.

Product	Affected Versions	Affected Features/Modules
AG/vxAG	ArrayOS AG 9.4.0.445 and earlier versions	System

Solution & Guidelines

For AG/vxAG series products, it is recommended to upgrade them to the latest version (AG 9.4.0.44x) to solve this vulnerability. Please contact Array Networks Customer Support to obtain the new ArrayOS AG version.

Workaround

In the meantime, if upgrading the AG/vxAG is not feasible, the following options could be used as a short-term emergency fix.

Enable URL filter in a virtual site with the following commands:

- CLI command: **filter on**
- CLI command: **filter url keyword deny “prelogin”**
- CLI command: **filter url keyword deny “runcli”**

Note: This could only be used as a short-term emergency fix. It cannot be used as a long-term solution as it may lead to serious system issues.

Any questions, please contact Array Networks Support via phone or e-mail.