Array Networks Security Advisory: System Service Buffer Overflow Vulnerability in AG Products

Revision History

Revision	Date	Description
V1.0	April 21, 2023	Initial Publication.

Overview

The system service buffer overflow vulnerability was discovered in AG products. A remote attacker can cause a buffer overflow in the system service process by sending specially crafted packets, and then execute arbitrary commands remotely.

Severity: Critical

Impact

The vulnerability allows an attacker to remotely execute arbitrary commands.

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
AG/vxAG	AG Rel_AG_9_4_0_484 and all previous versions

Solution & Guidelines

This issue will be fixed in the following versions:

For ArrayOS AG 9.4.0.484 and earlier versions, please upgrade to ArrayOS AG 9.4.0.485 and later versions.

Workaround

No temporary workaround.

1371 McCarthy Blvd. Milpitas, CA 95035 | Phone: (408) 240-8700 Toll Free: 1-877-99-ARRAY E-mail: support@arraynetworks.com | www.arraynetworks.com

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

1371 McCarthy Blvd. Milpitas, CA 95035 | Phone: (408) 240-8700 Toll Free: 1-877-99-ARRAY E-mail: support@arraynetworks.com | www.arraynetworks.com