Date: July 8, 2024

Revision	Date	Changes
1.0	July 8th, 2024	Initial release
1.1	September 24th, 2024	Update the fixed release info for affected products

The CVE-ID tracking this issue: CVE-2024-6387
CVSSv3.1 Base Score: 8.1 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H)
Common Weakness Enumeration: CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')
This vulnerability is being tracked by BUG973424(EOS) and BUG973802(WI-FI AP)

Description

Arista Networks is providing this security update in response to the OpenSSH security vulnerability CVE-2024-6387, named regreSSHion.

The vulnerability involves a signal handler race condition that can lead to a potential unauthenticated remote code execution in OpenSSH's server (sshd) in glibc-based Linux systems that grants full root access. It affects the default configuration and does not require user interaction, posing a significant exploit risk.

Affected OpenSSH Versions:

- OpenSSH < 4.4p1 is vulnerable to this signal handler race condition, if not backport-patched against CVE-2006-5051, or not patched against CVE-2008-4109, which was an incorrect fix for CVE-2006-5051;
- 4.4p1 <= OpenSSH < 8.5p1 is not vulnerable to this signal handler race condition
- 8.5p1 <= OpenSSH < 9.8p1 is vulnerable again to this signal handler race condition (because the "#ifdef DO_LOG_SAFE_IN_SIGHAND" was accidentally removed from sigdie()).

Arista Product Security Incident Response Teams are aware of, and are urgently investigating our product suites exposure to this issue. A current list of affected products is included below and Arista will update this advisory with information pending ongoing assessment.

Vulnerability Assessment

Affected Software

EOS release versions:

- 4.32.1F and below releases in the 4.32.x train only.
- 4.31.X and below are not impacted.

WI-FI Access Points versions:

- 17.0.0-236 and below versions in the 17.0 release
- 16.1 release train
- 16.0 release train

Awake Security versions:

- 5.1.2 and below releases in the 5.1.x train
- 5.0.6 and below releases in the 5.0.x train
- 4.2.5 and below releases in the 4.2.x train

Affected Platforms

Arista EOS-based products:

- 710 Series
- 720D Series
- 720XP/722XPM Series
- 750X Series
- 7010 Series
- 7010X Series
- 7020R Series
- 7130 Series running EOS
- 7150 Series
- 7160 Series
- 7170 Series
- 7050X/X2/X3/X4 Series
- 7060X/X2/X4/X5 Series
- 7250X Series
- 7260X/X3 Series
- 7280E/R/R2/R3 Series
- 7300X/X3 Series
- 7320X Series
- 7358X4 Series
- 7368X4 Series
- 7388X5 Series
- 7500E/R/R2/R3 Series
- 7800R3 Series
- CloudEOS
- cEOS-lab
- vEOS-lab
- AWE 5000 Series
- CloudVision eXchange, virtual or physical appliance

Arista Wireless Access Points:

- All AP models

Arista Network Detection and Response (NDR) Security Platform (Formerly Awake NDR):

- Arista NDR AVA Nucleus
- Arista NDR AVA Campus Nucleus

The following products are **NOT** affected by CVE-2024-6387:

- CloudVision CUE, virtual appliance or physical appliance
- CloudVision CUE cloud service delivery
- CloudVision AGNI
- CloudVision Portal, virtual appliance or physical appliance
- CloudVision as-a-Service
- Arista 7130 Systems running MOS
- Arista Converged Cloud Fabric and DANZ Monitoring Fabric (Formerly Big Switch Nodes for BCF and BMF)
- Arista Edge Threat Management - Arista NG Firewall and Arista Micro Edge (Formerly Untangle)
- Arista NetVisor OS, Arista NetVisor UNUM, and Insight Analytics (Formerly Pluribus)

Mitigation

Enhanced Access Control

Arista EOS-based products

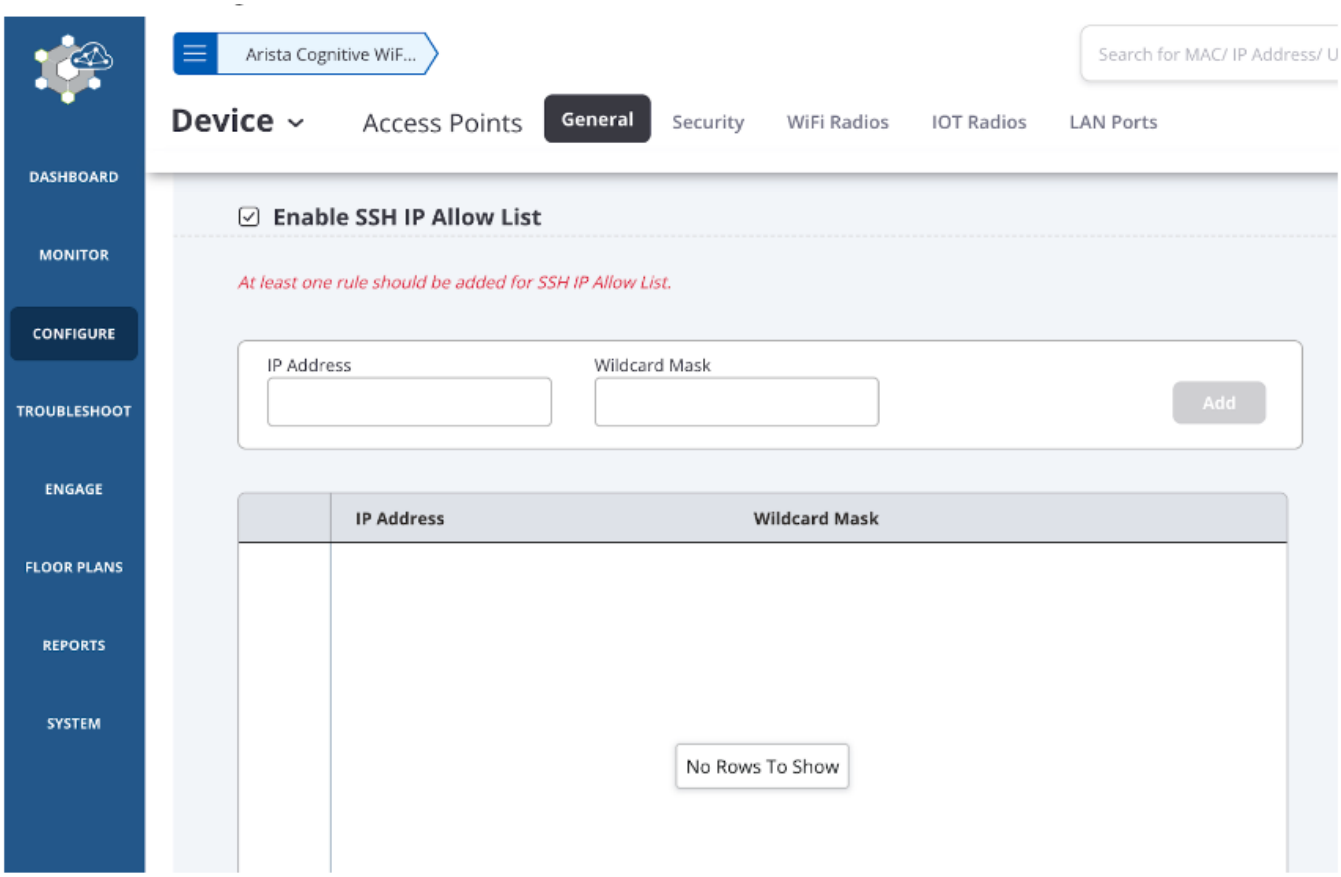
Enable SSH service ACLs to limit SSH access to minimize the attack risks.

```
ip access-list allowHosts4
   10 permit ip host <ipv4 address> any

ipv6 access-list allowHosts6
   10 permit ipv6 host <ipv6 address> any

management ssh
   ip access-group allowHosts4 in
   ipv6 access-group allowHosts6 vrf RED in
```

For more information about SSH service ACLs see Configuring Service ACLs and Displaying Status and Counters.

Arista Wireless Access Points

This workaround is to restrict SSH access to the AP from known IPs by defining the whitelist on CV-CUE, Configure --> Device --> AccessPoints --> General --> Enable SSH IP Allow List



Disable SSH Server Authentication Timeout

The workaround is to set LoginGraceTime to 0 to fix the signal handler race condition in OpenSSH.

Note: The LoginGraceTime mitigation has a side effect of removing protection from the malicious attackers attempting to tie up server resources by opening connections and leaving them idle indefinitely. This could lead to a denial-of-service (DoS) condition where legitimate users cannot connect because server resources are exhausted.

If such a DoS is attempted, ACLs should be added on the device or its connected switches and firewalls to limit the sources of malicious traffic until an upgrade to a patched release can be deployed.

Arista EOS-based products

```
switch(config)#management ssh
```

```
switch(config-mgmt-ssh)#no login timeout
```

Arista NDR Security Platform

The NDR ops team has deployed the OpenSSH timeout configuration change that mitigates the issue to all vulnerable managed appliances.

No user configuration is required.

Resolution

Arista EOS-based products

- 4.32.2F and later releases in the 4.32.x train

Arista Wireless Access Points

- 17.0.0-241 and later versions in the 17.0 release train
- 16.1.0-51.1004 and later versions in the 16.1 release train

Arista NDR Security Platform

- 5.2.3 and later releases in the 5.2.x train

Hotfix

The following hotfix can be applied to remediate CVE-2024-6387. The hotfix only applies to the EOS-based product for affected releases, namely 4.32.0F and 4.32.1F. All other affected products require upgrading to a release containing the fix (as listed above) or applying the mitigation as a temporary fix.

Note: Installing/uninstalling the SWIX will cause the SuperServer agent to restart, services may be unavailable for up to one minute. The existing session should not get interrupted but it's suggested to re-login after the hotfix installation.

Arista EOS-based products

- 4.32.1F and below releases in the 4.32.x train

Version: 1.0
URL: https://www.arista.com/support/advisories-notices/sa-download/?sa100-SecurityAdvisoryTamalpaisHotfix.swix

```
SWIX hash:(SHA512)
7766e19fa5ea607af77272c1a8363c7c9c10140cb7a7f99f6bc674b0bc91b808a571f600830856033a557
51580e30519640fe1a9583a1a6aebec86d184ec8f7f
```

For instructions on installation and verification of the hotfix patch, refer to the “managing eos extensions” section in the EOS User Manual. Ensure that the patch is made persistent across reboots by running the command ‘**copy installed-extensions boot-extensions**’.

References

- https://www.openssh.com/releasenotes.html
- https://www.qualys.com/2024/07/01/cve-2024-6387/regresshion.txt
- https://www.qualys.com/regresshion-cve-2024-6387/

For More Information

If you require further assistance, or if you have any further questions regarding this security notice, please contact the Arista Networks Technical Assistance Center (TAC) by one of the following methods:

Open a Service Request

Contact information needed to open a new service request may be found at: https://www.arista.com/en/support/customer-support