**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 |
| 1.2 | July 22nd, 2025 | Add CVE-2024-6409 affected info and update hotfix to version 2.0 which addresses both CVEs |
| 1.3 | August 1st, 2025 | Fix which releases the hotfix applies to (4.34.0, not 4.34.1) |
| 1.4 | September 29th, 2025 | Update hotfix to version 3.0 to fix 4.32.3M |
| 1.5 | June 16th, 2026 | Clarify Resolution section |

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)

The CVE-ID tracking this issue: CVE-2024-6409
CVSSv3.1 Base Score: 7.0 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:H)
Common Weakness Enumeration: CWE-364: Signal Handler Race Condition
This vulnerability is being tracked by BUG1137400(EOS)

## Description

Arista Networks is providing this security update in response to the OpenSSH security vulnerability CVE-2024-6387 named “regreSSHion” and CVE-2024-6409 that was found during a thorough audit of OpenSSH's signal handling after CVE-2024-6387 was disclosed.

CVE-2024-6387 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()).

CVE-2024-6409 is a vulnerability specific to Red Hat-derived distributions, including RHEL and its downstream variants, that is similar in nature to CVE-2024-6387 but affecting a different signal-handling path. The flaw involves the unsafe use of non-async-signal-safe functions inside a signal handler, which can be exploited by a remote unauthenticated attacker to potentially perform a remote code execution (RCE) as an unprivileged user running the sshd server.

**Affected OpenSSH Versions:**

- 8.7p1 and 8.8p1 in Red Hat Enterprise Linux 9

# Vulnerability Assessment

## Affected Software

The following product releases **are** affected for CVE-2024-6387

### 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
- 16.1.0-51.903 and below versions in the 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

The following product releases **are** affected for CVE-2024-6409

### EOS release versions:

- 4.34.0F and below releases in the 4.34.x train
- 4.33.3.1F and below releases in the 4.33.x train
- 4.32.5.1M and below releases in the 4.32.x train
- 4.31.X and below are not impacted.

## Affected Platforms

### Arista EOS-based products (CVE-2024-6387 and CVE-2024-6409):

- 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
- 7700R4 Series
- 7800R3/R4 Series
- CloudEOS
- cEOS-lab
- vEOS-lab
- AWE 5000 Series
- CloudVision eXchange, virtual or physical appliance

### Arista Wireless Access Points (CVE-2024-6387 only):

- All AP models

### Arista Network Detection and Response (NDR) Security Platform (Formerly Awake NDR) (CVE-2024-6387 only):

- Arista NDR AVA Nucleus

- Arista NDR AVA Campus Nucleus

The following products are **NOT** affected by CVE-2024-6387 or CVE-2024-6409:

- 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

For both CVE-2024-6387 and CVE-2024-6409, the following options can be used to mitigate those vulnerabilities.

## Enhanced Access Control

### Arista EOS-based products

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

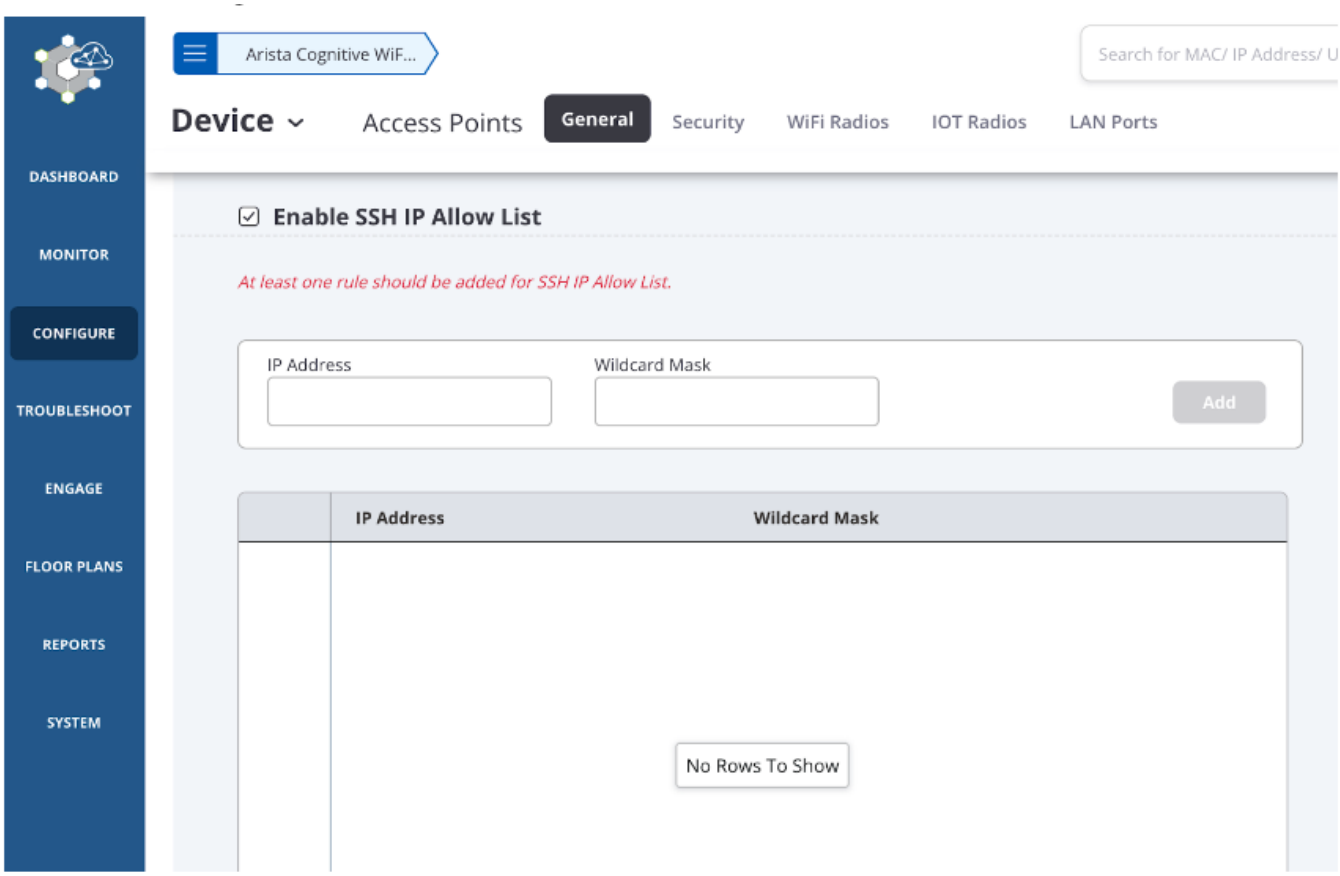
```
ip access-list allowHosts4
   10 permit ip host <ipv4 address> any

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

CVE-2024-6387 has been fixed in the following product releases:

### 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

CVE-2024-6409 has been fixed in the following product releases:

### Arista EOS-based products

- 4.34.1F and later releases in the 4.34.x train
- 4.33.4M and later releases in the 4.33.x train
- 4.32.6M and later releases in the 4.32.x train

**Vulnerability Scanner Advisory:** Certain security scanners might incorrectly flag the fixed versions in the 4.34.1F, 4.33.x, and 4.32.x release trains as susceptible to CVE-2024-6387 and CVE-2024-6409. These results are false positives. This occurs because the official security patches were backported into the existing OpenSSH packages without incrementing the version string. Following standard enterprise Linux protocols (consistent with Red Hat and AlmaLinux), this methodology prioritizes system stability by integrating critical code repairs while maintaining established versioning schemes. The underlying vulnerabilities have been fully resolved in these releases regardless of the reported OpenSSH version number.

## Hotfix

The following hotfix can be applied to remediate CVE-2024-6387 and CVE-2024-6409. The hotfix only applies to the EOS-based product for affected releases listed below. 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
- 4.32.3M
- 4.32.5M and 4.32.5.1M
- 4.33.2F, 4.33.2.1F, 4.33.3F, and 4.33.3.1F
- 4.34.0F

Version: 3.0
URL: https://www.arista.com/en/support/advisories-notices/sa-download?sa100-SecurityAdvisory100_CVE-2024-6387_CVE-2024-6409_Hotfix_V3.swix

```
SWIX hash:(SHA512)
59393ecf84d4e4bb416b8dd2f9e04143f57fc7a39a3b7588758c016217458c5a598795a798c6d4085b93d
4e23c644795b09dce3ed8da59da48641f2a36cb74f9
```

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/
- https://access.redhat.com/security/cve/cve-2024-6409

## 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