Date: April 7, 2026

Revision	Date	Changes
1.0	April 7th, 2026	Initial release

The CVE-ID tracking this issue: CVE-2025-31133
CVSSv3.1 Base Score: 7.8/10 (CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H)
CVSS:4.0 Base Score: 7.3/10
(CVSS:4.0/AV:L/AC:L/AT:P/PR:L/UI:A/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H)
Common Weakness Enumeration: CWE-61: UNIX Symbolic Link (Symlink) Following

The CVE-ID tracking this issue: CVE-2025-52565
CVSSv3.1 Base Score: 7.5/10 (CVSS:3.1/AV:L/AC:H/PR:L/UI:R/S:C/C:H/I:H/A:H)
CVSS:4.0 Base Score: 8.4/10
(CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:P/VC:N/VI:H/VA:N/SC:H/SI:H/SA:H)
Common Weakness Enumeration: CWE-61: UNIX Symbolic Link (Symlink) Following

The CVE-ID tracking this issue: CVE-2025-52881
CVSSv3.1 Base Score: 7.5/10 (CVSS:3.1/AV:L/AC:H/PR:L/UI:R/S:C/C:H/I:H/A:H)
CVSS:4.0 Base Score: 7.3/10
(CVSS:4.0/AV:L/AC:L/AT:P/PR:L/UI:A/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H)
Common Weakness Enumeration: CWE-61: UNIX Symbolic Link (Symlink) Following

These vulnerabilities are being tracked by BUG1342998 (EOS) and BUG1471007 (MOS).

Description

Arista Networks is providing this security advisory regarding three high-severity vulnerabilities identified in runC, the lightweight, command-line tool for spawning and running containers. These vulnerabilities present a potential risk of allowing malicious actors to circumvent container isolation mechanisms.

For EOS-based products, these issues are strictly isolated to the cEOS-lab platform and the optional, standalone Docker SWIX extension available via the Download portal under Extensions section. The standard core EOS release images do not ship with this component and remain secure.

- CVE-2025-31133
  The vulnerability involves an attacker swapping the container's /dev/null with a symbolic link to a sensitive host file just as runC is setting up the mask. runC then accidentally overwrites the sensitive host file instead of masking it, which can cause host information disclosure, host denial of service, and container escape.
- CVE-2025-52565
  Similar to CVE-2025-31133, the vulnerability exists where the /dev/pts/$n bind mount to /dev/console can be exploited through a symbolic link during container initialization.

Insufficient validation allows attackers to redirect this mount and gain write access to protected procfs files, potentially leading to container breakouts.
- CVE-2025-52881:
  The vulnerability uses a race condition with shared mounts to redirect runC writes to /proc files, bypassing Linux Security Module (LSM) labels. Attackers can trick runC into writing fake procfs files instead of security label files. This critically allows redirecting arbitrary sysctl writes to dangerous files like /proc/sysrq-trigger (to crash the system) or /proc/sys/kernel/core_pattern (to escape the container). The flaw affects all runC writes to /proc, including sysctls and security labels.

Arista Engineering and PSIRT teams are actively developing fixes to remaining affected products, and will continue to update this advisory when more information is available.

Vulnerability Assessment

Affected Software

cEOS Version

- 4.35.2F and below releases in the 4.35.x train
- 4.34.4M and below releases in the 4.34.x train
- 4.33.7M and below releases in the 4.33.x train
- 4.32.9M and below releases in the 4.32.x train
- 4.31.x and all earlier releases

Docker SWIX Extension Versions associated with the below EOS versions (Available in the Arista Download portal under Extensions section)

- 4.35.2F and below releases in the 4.35.x train
- 4.34.4M and below releases in the 4.34.x train
- 4.33.7M and below releases in the 4.33.x train
- 4.32.9M and below releases in the 4.32.x train
- 4.31.x and all earlier releases

Arista 7130 Systems running MOS

- MOS-0.39.12 and below releases

Affected Platforms

The following products are affected by this vulnerability:

- Arista EOS-based products:
  - cEOS-lab
- ***Unaffected by default***.

For all other Arista EOS-based products listed below, the below platforms are only affected when Docker SWIX extension is installed:

  - 710 Series
  - 720D Series
  - 720XP/722XPM Series
  - 750X Series
  - 7010 Series
  - 7010X Series
  - 7020R/R4 Series
  - 7130 Series running EOS
  - 7150 Series
  - 7160 Series
  - 7170 Series
  - 7050X/X2/X3/X4 Series
  - 7060X/X2/X4/X5/X6 Series
  - 7250X Series
  - 7260X/X3 Series
  - 7280E/R/R2/R3/R4 Series
  - 7300X/X3 Series
  - 7320X Series
  - 7358X4 Series
  - 7368X4 Series
  - 7388X5 Series
  - 7500E/R/R2/R3 Series
  - 7800R3/R4 Series
  - 7700R4 Series
  - AWE 5000 Series
  - AWE 7200R Series
  - CloudEOS
  - vEOS-lab
  - CloudVision eXchange, virtual or physical appliance
- Arista 7130 Systems running MOS

The following product versions and platforms are **not** affected by this vulnerability:

- Arista Wireless Access Points
- CloudVision CUE, virtual appliance or physical appliance
- CloudVision CUE cloud service delivery
- CloudVision Portal, virtual appliance or physical appliance
- CloudVision as-a-Service
- CloudVision AGNI
- Arista Converged Cloud Fabric (formerly Big Switch BCF)
- Arista DANZ Monitoring Fabric (formerly Big Switch BMF)
- Arista Network Detection and Response (NDR) Security Platform (Formerly Awake NDR)

- Arista Edge Threat Management - Arista NG Firewall and Arista Micro Edge (Formerly Untangle)
- Arista NetVisor OS, Arista NetVisor UNUM, and Insight Analytics (Formerly Pluribus)
- VeloCloud Orchestrator (Formerly VeloCloud Orchestrator by Broadcom)
- VeloCloud Gateway (Formerly VeloCloud Gateway by Broadcom)
- VeloCloud Edge (Formerly VeloCloud Edge by Broadcom)

Required Configuration for Exploitation

Arista EOS-based products

In order to be vulnerable to CVE-2025-31133, CVE-2025-52565 or CVE-2025-52881, the following condition must be met:

The docker runtime SWIX extension must be installed with the affected release versions for **non-cEOS** products.
Run "***show extensions***" and look for any extensions with "***...-docker.swix***"
An example of this is shown below:

```
switch# show extensions
Name                        Version/Release Status Extension
--------------------------- --------------- ------ ---------
EOS64-4.35.1F-docker.swix  27.3.1/1.el9    A, I           8

A: available | NA: not available | I: installed | F: forced | B: install at boot
S: valid signature | NS: invalid signature
The extensions are stored on internal flash (flash:)
```

Alternatively, for all EOS-based products including cEOS, the docker RPM release version must be less than v28.5.2 to be vulnerable. This can be checked by running the following CLI show command:

```
switch# show version detail | grep docker-ce
docker-ce            27.3.1          1.el9
docker-ce-cli        27.3.1          1.el9
docker-ce-rootless-extras 27.3.1          1.el9
```

Arista 7130 Systems running MOS

MOS devices are vulnerable to CVE-2025-31133, CVE-2025-52565 and CVE-2025-52881 by default, and no specific configuration is necessary.

Indicators of Compromise

The following checks may help identify any related Indicators of Compromise for all affected products:

- Presence of symlinks that specifically target /dev/null, /dev/console or /dev/pts/* that point back to sensitive host files
- Docker daemon logs that contain unexpected mount operations and/or mount failures during container startup, as well as runC panics, stack traces or errors mentioning /dev/null, /dev/console, /dev/pts/* or dangling symlinks

Mitigation

To prevent the exploitation of CVE-2025-31133, CVE-2025-52565 or CVE-2025-52881, it's critical to make sure that all container images deployed originate from verified and trusted sources. Since those vulnerabilities rely on manipulating the container's root filesystem to create a race condition during initialization, using unvetted images poses a high risk of host-level compromise.

Resolution

CVE-2025-31133, CVE-2025-52565 or CVE-2025-52881 has been fixed in the following product releases:

Arista EOS-based products

cEOS Version

- 4.35.3F and later releases in the 4.35.x train
- 4.34.5M and later releases in the 4.34.x train
- 4.33.x has the fix under development and will be updated when released
- 4.32.9M and later releases in the 4.32.x train

Docker SWIX Extension Versions associated with the below EOS versions (Available in the Arista Download portal under Extensions section):

- 4.35.3F and later releases in the 4.35.x train
- 4.34.5M and later releases in the 4.34.x train
- 4.33.x has the fix under development and will be updated when released
- 4.32.9M and later releases in the 4.32.x train

Arista 7130 Systems running MOS

- MOS-0.39.13 and later releases

References

- https://nvd.nist.gov/vuln/detail/CVE-2025-52881
- https://nvd.nist.gov/vuln/detail/CVE-2025-52565
- https://nvd.nist.gov/vuln/detail/CVE-2025-31133
- https://arista.my.site.com/AristaCommunity/s/article/managing-containers-on-eos-container-manager

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