Date: November 11, 2025

Revision	Date	Changes
1.0	November 11, 2025	Initial release

The CVE-ID tracking this issue: CVE-2025-8870
CVSS:3.1 Base Score 4.9 (CVSS:3.1/AV:P/AC:H/PR:N/UI:N/S:C/C:N/I:N/A:H)
CVSS:4.0 Base Score 5.6
(CVSS:4.0/AV:P/AC:L/AT:P/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:H)
Common Weakness Enumeration: CWE-248: Uncaught Exception
This vulnerability is being tracked by BUG 1206724

Description

On affected platforms running Arista EOS, certain serial console input might result in an unexpected reload of the device.

This issue was discovered internally by Arista and is not aware of any malicious uses of this issue in customer networks.

Vulnerability Assessment

Affected Software

EOS Versions

- 4.34.2FX version only.

Affected Platforms

The following products **are** affected by this vulnerability:

- Arista EOS-based products:
  - 710X Series (CCS-710XP-12TH-2S)

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

- Arista EOS-based products:
  - 710 Series
  - 720D Series
  - 720XP/722XPM Series
  - 750X Series
  - 7010/7010X Series

    - 7020R 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
    - cEOS-lab
    - vEOS-lab
    - CloudVision eXchange, virtual or physical appliance
- 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 7130 Systems running MOS
- 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

In order to be vulnerable to CVE-2025-8870, both of the following conditions must be met:

1. An attacker must have a serial interface connection to the device or access to remotely access the console via the console port. Network remote access does not cause this issue.

AND

2. Device must be using the Synopsys Designware serial model:

```
#bash dmesg | grep "Synopsys DesignWare"
[    1.287358] 10200000.serial: ttyS0 at MMIO 0x10200000 (irq = 15, base_baud
= 15625000) is a Synopsys DesignWare
[    1.287845] 10201000.serial: ttyS1 at MMIO 0x10201000 (irq = 164, base_baud
 = 15625000) is a Synopsys DesignWare
```

Indicators of Compromise

This vulnerability may lead to an unexpected system reload.

Run '**show reload cause**' and inspect logs for the highlighted section as illustrated below:

```
show reload cause
Reload Cause 1:
-------------------
The system rebooted due to a watchdog caused by a kernel panic

Reload Time:
------------
Reload occurred at Tue Jul 22 22:14:21 2025 PDT.

Recommended Action:
-------------------
This may indicate a software or hardware problem.
Contact your customer support representative.

Debugging Information:
------------------------------
NOTE: Displaying last 2000 lines of crash log
…
[  855.830755] [   T4280] ttyS ttyS0: 2 input overrun(s)
[  856.024336] [      C0] watchdog: BUG: soft lockup - CPU#0 stuck for 21s! [swapper/
0:0]
[  856.024366] [      C0] Modules linked in: fifo_dma(PO) sch_prio …
```

```
[  856.024732] [      C0]  arch_local_irq_enable+0xc/0x14
[  856.024737] [      C0]  __irq_exit_rcu+0x80/0x98
[  856.024742] [      C0]  irq_exit+0x18/0x28
[  856.024749] [      C0]  __handle_domain_irq+0x78/0xa8
[  856.024754] [      C0]  gic_handle_irq+0xa8/0xcc
[  856.024759] [      C0]  el1_irq+0xcc/0x180
[  856.024766] [      C0]  arch_cpu_idle+0x18/0x28
[  856.024772] [      C0]  default_idle_call+0x48/0x68
[  856.024778] [      C0]  do_idle+0x120/0x224
[  856.024783] [      C0]  cpu_startup_entry+0x2c/0x44
[  856.024789] [      C0]  rest_init+0xd8/0xe8
[  856.024797] [      C0]  arch_call_rest_init+0x18/0x24
[  856.024802] [      C0]  start_kernel+0x544/0x57c
[  856.024808] [      C0] Kernel panic - not syncing: softlockup: hung tasks
```

Mitigation

The mitigation is to limit access to the serial console.

Resolution

The recommended resolution is to upgrade to a remediated software version at your earliest convenience. Arista recommends customers move to the latest version of each release that contains all the fixes listed below. For more information about upgrading see EOS User Manual: Upgrades and Downgrades

CVE-2025-8870 has been fixed in the following releases:

- 4.35.0F and later releases

Hotfix

There is no hotfix for this issue.

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