Date: February 14, 2023

Revision	Date	Changes
1.0	February 14th, 2023	Initial release
1.1	February 22nd, 2023	Update the Hotfix SWIX

The CVE-ID tracking this issue: CVE-2023-24509
CVSSv3.1 Base Score: 9.3 (CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)
Common Weakness Enumeration: CWE-269 Improper Privilege Management
This vulnerability is being tracked by BUG 723401

Description

On affected modular platforms running Arista EOS equipped with both redundant supervisor modules and having the redundancy protocol configured with RPR or SSO, an existing unprivileged user can login to the standby supervisor as a root user, leading to a privilege escalation. Valid user credentials are required in order to exploit this vulnerability.

Arista would like to acknowledge and thank Marc-André Labonté, Senior Information Security Analyst at Desjardins for responsibly reporting CVE-2023-24509.

Arista is not aware of any malicious uses of this issue in customer networks.

Vulnerability Assessment

Affected Software

EOS Versions

- 4.28.3M and below releases in the 4.28.x train
- 4.27.6M and below releases in the 4.27.x train
- 4.26.8M and below releases in the 4.26.x train
- 4.25.9M and below releases in the 4.25.x train
- 4.24.10M and below releases in the 4.24.x train
- 4.23.13M and below releases in the 4.23.x train

Affected Platforms

The following products are affected by this vulnerability:

Arista EOS-based products on modular switches with redundant supervisor modules:

- 755X Series
- 758X Series
- 7304X Series

- 7324X Series
- 7304X3 Series
- 7308X Series
- 7328X Series
- 7304X3 Series
- 7316X Series
- 7504R/R3 Series
- 7508R/R3 Series
- 7512R/R3 Series
- 7516R Series
- 7804R3 Series
- 7808R3 Series
- 7812R3 Series
- 7816R3 Series

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

- Arista EOS-based products not listed above
- Arista modular switches with a single supervisor module
- Arista Wireless Access Points
- CloudVision WiFi, virtual appliance or physical appliance
- CloudVision WiFi cloud service delivery
- 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 Network Detection and Response (NDR) Security Platform (Formerly Awake NDR)
- Arista Edge Threat Management (Formerly Arista NG Firewall and Arista Micro Edge)
- Arista Unified Cloud Fabrics - (Formerly Pluribus Netvisor One)

Required Configuration for Exploitation

In order to be vulnerable to CVE-2023-24509, the following conditions must be met:

Two supervisor modules must both be inserted and active. To determine the status of the supervisor modules,

```
switch#show module
Module  Ports Card Type                 Model            Serial No.
------- ----- ------------------------ ---------------- -----------
1       3     DCS-7500-SUP2 Supervisor DCS-7500-SUP2    SSJ17133450
2       2     Standby supervisor       DCS-7500-SUP2    SSJ17133441

Module  Status  Uptime  Power off reason
```

```
------- ------- ------- ----------------
1       Active  0:24:58 N/A
2       Standby 0:24:58 N/A
```

Supervisor redundancy protocol must be configured with RPR(Route Processor Redundancy) or SSO (Stateful Switchover) on the switch. To determine the state and the current redundancy protocol of both supervisors on the switch,

```
switch#show redundancy status
  my state = ACTIVE
peer state = STANDBY WARM
      Unit = Primary
   Unit ID = 1

Redundancy Protocol (Operational) = Route Processor Redundancy
Redundancy Protocol (Configured) = Route Processor Redundancy
Communications = Up
Ready for switchover

  Last switchover time = 7:23:56 ago
Last switchover reason = Supervisor has control of the active supervisor lock
```

Indicators of Compromise

This vulnerability may lead to privilege escalation issues. Unrecognized user activities in “/var/log/secure” may be an indication of the issue.

Any unrecognized login can also be an indication of the issue.

```
#show user detail
Session       Username       Roles                TTY        State       Duration
  Auth        Remote Host
------------- -------------- -------------------- ---------- ----------- -------------
- ----------- --------------
21            admin          network-
admin       con0       E           0:43:56        local
25            hacker         network-
operator    vty4       E           0:03:20        local       10.0.2.3
```

Mitigation

The workaround is to disable “ssh” CLI command in unprivileged mode on the SSH client devices by using command authorization. This can be done with Role-Based Access Control (RBAC).

If the “ssh” CLI command is currently used to connect to a remote host, the destination address can be added to an allowlist with RBAC.

More details for how to use RBAC can be found on the Arista TOI pages.

https://www.arista.com/en/support/toi/eos-4-18-0f/13861-tacacs-rbac

https://www.arista.com/en/support/toi/eos-4-18-0f/13834-radius-vsas

https://www.arista.com/en/um-eos/eos-user-security#concept_dyv_1pk_cnb

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.

CVE-2023-24509 has been fixed in the following releases:

- 4.28.4M and later releases in the 4.28.x train
- 4.27.7M and later releases in the 4.27.x train
- 4.26.9M and later releases in the 4.26.x train
- 4.25.10M and later releases in the 4.25.x train
- 4.24.11M and later releases in the 4.24.x train

Hotfix

The following hotfix can be applied to remediate CVE-2023-24509. The hotfix only applies to the releases listed below and no other releases. All other versions require upgrading to a release containing the fix (as listed above).:

- 4.28.3M and below releases in the 4.28.x train
- 4.27.6M and below releases in the 4.27.x train
- 4.26.8M and below releases in the 4.26.x train
- 4.25.9M and below releases in the 4.25.x train
- 4.24.10M
- 4.23.13M

Note: Installing/uninstalling the SWIX will cause ConfigAgent to restart and disconnect existing CLI sessions.

Version: 1.0

URL: SecurityAdvisory82_CVE-2023-24509_Hotfix.swix

SWIX hash:

```
(SHA-512)7833ab99e11cfea1ec28c09aedffd062cfc865a20a843ee6184caff1081e7
48c8a02590644d0c7b0e377027379cbaadc8b1a70d1c37097bf98c1bedb429dca56
```

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'.

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

By email: support@arista.com

By telephone: 408-547-5502 ; 866-476-0000

Contact information needed to open a new service request may be found at:

https://www.arista.com/en/support/customer-support