Date: August 23, 2023

Revision	Date	Changes
1.0	August 23, 2023	Initial release

The CVE-ID tracking this issue: CVE-2023-3646
CVSSv3.1 Base Score: 5.9 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H)
Common Weakness Enumeration: CWE-125 Out-of-bounds Read
This vulnerability is being tracked by BUG829136, which is triggered by BUG765111

Description

On affected platforms running Arista EOS with mirroring to multiple destinations configured, an internal system error may trigger a kernel panic and cause system reload.

CVE-2023-3646 Is tracked by BUG829136. In order to be vulnerable to the CVE a system must already be impacted by BUG765111, which is a non CVE known issue.

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

Vulnerability Assessment

Affected Software

EOS Versions

- 4.28.2F through 4.28.5.1M releases in the 4.28.x train
- 4.29.1F and below releases in the 4.29.x train

Affected Platforms

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

- Arista EOS-based products:
    - 7280R3 Series
    - 7289R3 Series
    - 7500R3 Series
    - 7800R3 Series

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

- Arista EOS Based Products

    - 710P 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 Series
    - 7300X/X3 Series
    - 7320X Series
    - 7358X4 Series
    - 7368X4 Series
    - 7388X5 Series
    - 7500E/R/R2 Series
    - CloudEOS
    - cEOS-lab
    - vEOS-lab
    - AWE 5000 Series
- Arista Wireless Access Points
- CloudVision WiFi, virtual appliance or physical appliance
- CloudVision WiFi cloud service delivery
- CloudVision eXchange, virtual or physical appliance
- CloudVision Portal, virtual appliance or physical appliance
- CloudVision as-a-Service
- CloudVision AGNI
- 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 - Arista NG Firewall and Arista Micro Edge (Formerly Untangle)

Required Configuration for Exploitation

CVE-2023-3646 Is tracked by BUG829136. In order to be vulnerable to the CVE a system must already be impacted by BUG765111, which is a non CVE known issue. In order to be impacted by BUG765111, the following conditions must be met:

Mirroring to multiple destinations must be configured:

```
switch(config)#show monitor session

Session s1
------------------------

Sources:

Both Interfaces:        Et1/1

Destination Ports:

    Et9/1 :  active
    Et10/1 :  active
```

In the above example two destinations, Et9/1 and Et10/1, are configured.

Mirroring config must be added with mirror destination being ethernet port, example:

```
switch # show running-config | section monitor
monitor session APCON destination Ethernet54/1
```

In the above example the argument after destination is an Ethernet port.

Indicators of Compromise

This vulnerability may lead to a kernel panic and cause system reload.

The following kernel message would appear in the output of “**show reload cause**” or the kernelcrash log (i.e. /mnt/flash/debug/kernelcrash.last, this requires bash access) which indicates the issue:

```
[ 4733.949388] BUG: unable to handle kernel NULL pointer dereference at 0000000000000
001
[ 4734.043395] PGD 0 P4D 0
[ 4734.043399] Oops: 0000 [#1] PREEMPT SMP NOPTI
[ 4734.043403] CPU: 1 PID: 0 Comm: swapper/1 Kdump: loaded Tainted: P           O
  4.19.142.Ar-28837868.4283M #1
[ 4734.043404] Hardware name: Arista Woodpecker/Woodpecker, BIOS Aboot-
norcal9-9.0.3-4core-14223577 11/13/2019
```

```
[ 4734.043413] RIP: 0010:fab_sand_hdrinfo+0x226a/0x2f92 [sand_dma]
[ 4734.043415] Code: 00 00 8b 85 a0 fd ff ff 2d ff 03 00 00 83 f8 0f 76 2e 66 83 3d 1
a b0 0c 00 00 74 4f 48 8b b5 f8 fd ff ff 48 8b 85 f8 fd ff ff <8a> 5e 01 0f b6 00 89
da c1 e0 02 c0 ea 06 83 e0 0c 0f b6 d2 09 d0
[ 4734.043416] RSP: 0018:ffff888fee2836c0 EFLAGS: 00010202
[ 4734.043418] RAX: 0000000000000000 RBX: 0000000000000000 RCX: ffff888c180ac08f
[ 4734.043419] RDX: ffffffffa0335330 RSI: 0000000000000000 RDI: ffff888c180ac078
[ 4734.043421] RBP: ffff888fee283990 R08: 00000000010001c0 R09: 0000000000000000
[ 4734.043422] R10: 000fffffffff000 R11: ffff888e7a1841d0 R12: ffff888c180ac082
[ 4734.043423] R13: 000000000000002c R14: ffff888fee283ce0 R15: ffff888cc078b500
[ 4734.043425] FS:  0000000000000000(0000) GS:ffff888fee280000(0000) knlGS:0000000000
000000
[ 4734.043426] CS:  0010 DS: 0000 ES: 0000 CR0: 0000000080050033
[ 4734.043427] CR2: 0000000000000001 CR3: 0000000ed1520000 CR4: 00000000001406e0
[ 4734.043429] Call Trace:
[ 4734.043431]  <IRQ>
[ 4734.043437]  ? ip_route_input_slow+0x45b/0x9f8
[ 4734.043442]  ? ip_route_input_rcu+0x1e0/0x209
[ 4734.043445]  ? skb_free_head+0x28/0x2a

...

[ 4734.043638] CS:  0010 DS: 0000 ES: 0000 CR0: 0000000080050033
[ 4734.043639] CR2: 0000000000000001 CR3: 0000000ed1520000 CR4: 00000000001406e0
[ 4734.043641] Kernel panic - not syncing: Fatal exception in interrupt
[ 4734.119914] Kernel Offset: disabled
[ 4734.161753] panic_event_handler: unable to lock eeprom
```

The above log lines indicate that sand-dma caused a kernel panic. These logs will be present after reboot.

To determine if BUG765111 is impacting the system:
Run the following CLI command:

```
#platform fap <fapName> diag dump chg ETPPA_PER_PORT_TABLE 0 1
```

If neither "**PRP_CONTEXT_PORT_PROFILE=1" nor "FWD_CODE_PORT_PROFILE=2"** are present then BUG765111 is impacting the system and it is possible for CVE-2023-3646 to occur.

Example of a system **not** impacted by BUG765111:

```
#platform fap Fap0 diag dump chg ETPPA_PER_PORT_TABLE 0 1
Fap0 diag dump chg ETPPA_PER_PORT_TABLE 0 1:
ETPPA_PER_PORT_TABLE.ETPPA0[0]: <PRP_CONTEXT_PORT_PROFILE=1
,PORT_EM_ACC_CMD=8,LLVP_PROFILE=1,FWD_CODE_PORT_PROFILE=2,ECC=0x28,>
```

Example of a system impacted by BUG765111:

```
#platform fap Fap0 diag dump chg ETPPA_PER_PORT_TABLE 0 1
Fap0 diag dump chg ETPPA_PER_PORT_TABLE 0 1:
ETPPA_PER_PORT_TABLE.ETPPA0[0]: <PORT_EM_ACC_CMD=8,LLVP_PROFILE=1,ECC=0x2b,>
```

Here **PRP_CONTEXT_PORT_PROFILE=1** and **FWD_CODE_PORT_PROFILE=2** are **not** present which indicates the system is impacted by BUG765111.

Mitigation

The suggestion to prevent this issue is to remove any mirroring config

```
#show monitor session
No sessions created
```

This example confirms that the system does not have any mirroring config present which will prevent this issue from occurring.

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-2023-3646 has been fixed in the following releases:

- 4.28.6M and later releases in the 4.28.x train
- 4.29.2F and later releases in the 4.29.x train

Hotfix

The following hotfix can be applied to remediate CVE-2023-3646. 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):

- 4.28.2F through 4.28.5.1M releases in the 4.28.x train
- 4.29.1F and earlier releases in the 4.29.X train

Note: Installing/uninstalling the Hotfix will result in a restart of the SandFapNi agent and an associated reprogramming of the switch chip. This process could result in outages from 5-20 minutes, depending on the number of active ports in the particular system.

To determine which hotfix to use, run “**show version**” from the CLI and refer to the “Architecture” Field.

Version: 1.0

URL: SecurityAdvisory88_CVE-2023-3646_Hotfix_i686.swix

```
SWIX hash:(SHA-512)
9c01d1bc1d657879e1a1b657a8c0dab090d589efc3f2c64e9cac1ae0356fce14496809893bffb0892b150
5f8b4ee25cad0064bd7315ba6737dc5fdb200539f1a
```

URL: SecurityAdvisory88_CVE-2023-3646_Hotfix_x86_64.swix

```
SWIX hash:(SHA512)
98e98c2c34f81df4da3e4068ac9a81191f4c6ef1acab884972d092c79a7495e00d9a25c8713620d3e25b4
699f777810a627634eb8078dcbbb19317ed27a9b0d5
```

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