April 26th, 2022

Revision	Date	Changes
1.0	April 26th, 2022	Initial release
1.1	May 16th, 2022	Updated hotfix information

The CVE-ID tracking this issue: CVE-2021-28510
CVSSv3.1 Base Score: 5.3 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L)
Common Weakness Enumeration: CWE-400 (Uncontrolled Resource Consumption)
This vulnerability is being tracked by BUG638107

Description

For certain systems running EOS, a Precision Time Protocol (PTP) packet of a management/signaling message with an invalid Type-Length-Value (TLV) causes the PTP agent to restart. Repeated restarts of the service will make the service unavailable.

The impact of this issue is that a remote attacker can make the PTP service unavailable. If this happens, the switch will fail to provide PTP time synchronization services to the devices downstream, leading to the degrading of the time maintained by the downstream devices.

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

- 4.27.1 and below releases in the 4.27.x train
- 4.26.4 and below releases in the 4.26.x train
- 4.25.6 and below releases in the 4.25.x train
- 4.24.8 and below releases in the 4.24.x train
- 4.23.10 and below releases in the 4.23.x train
- 4.22.x train

Affected Platforms

The following products are affected by this vulnerability:

Any platform supporting PTP.

Arista EOS-based products:

- 7020R Series
- 7050X/X2/X3 series
- 7060X/X2/X4 series
- 7150 series
- 7170 series
- 720XP series
- 7250X series
- 7260X/X3 series
- 7280E/R/R2 series
- 7300X/X3 series
- 7320X series
- 7368 / X4 series
- 7500E/R/R2 series
- 7500R3 Series
- 7800R3 Series
- 7280R3 Series

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

- Arista EOS-based products:
  - 7010 series
  - 7160 series
  - 750X series
- 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)
- Awake Security Platform

Required Configuration for Exploitation

In order to be vulnerable to CVE-2021-28510 the following conditions must be be met:

PTP should be enabled on the switch. To determine if PTP is enabled on the switch,

```
switch# show ptp
PTP Mode: Boundary Clock
PTP Profile: Default ( IEEE1588 )
Clock Identity: 0x74:83:ef:ff:ff:00:23:b1
Grandmaster Clock Identity: 0x00:00:00:00:00:00:00:00
Number of slave ports: 1
Number of master ports: 4
Offset From Master (nanoseconds): 0
Mean Path Delay (nanoseconds): 0
Steps Removed: 0
Skew (estimated local-to-master clock frequency ratio): 1.0
```

Indicators of Compromise

This issue causes the PTP agent to crash. If you are seeing a high number of syslog messages stating that the PTP agent is being restarted, this issue is potentially being exploited.

```
Apr 12 02:32:08 ok312 ProcMgr-worker: %PROCMGR-6-PROCESS_TERMINATED: '
Ptp' (PID=17476, status=15) has terminated.
Apr 12 02:32:08 ok312 ProcMgr-worker: %PROCMGR-6-PROCESS_RESTART: Rest
arting 'Ptp' immediately (it had PID=17476)
Apr 12 02:32:08 ok312 ProcMgr-worker: %PROCMGR-7-PREDECESSOR_WAITING:
New instance of Ptp (PID=17833): waiting for reaping of predecessor (P
ID=17476)
Apr 12 02:32:08 ok312 ProcMgr-worker: %PROCMGR-7-PREDECESSOR_GONE: New
 instance of Ptp (PID=17833): predecessor (PID=17476) has been reaped.
Apr 12 02:32:08 ok312 ProcMgr-worker: %PROCMGR-6-PROCESS_STARTED: 'Ptp
' starting with PID=17833 (PPID=3067) -- execing '/usr/bin/Ptp'
Apr 12 02:32:08 ok312 Ptp: %AGENT-6-INITIALIZED: Agent 'Ptp' initializ
ed; pid=17833
```

Mitigation

Install ACL rules to drop PTP packets from untrusted sources. Best practice is to block access to untrusted (non-management) networks.

```
ptp ip access-group ptpAcl in
<--------OUTPUT OMITTED FROM EXAMPLE--------->
!
ip access-list ptpAcl
```

```
   10 deny ip host 10.10.10.1 any
```

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-2021-28510 has been fixed in the following releases:

- 4.27.2 and later releases in the 4.27.x train
- 4.26.5 and later releases in the 4.26.x train
- 4.25.7 and later releases in the 4.25.x train
- 4.24.9 and later releases in the 4.24.x train
- 4.23.11 and later releases in the 4.23.x train

For immediate remediation until EOS can be upgraded, the following hotfix is available.

Hotfix

The following hotfix can be applied to remediate CVE-2021-28510. The hotfix applies only to 4.23.10 and no other releases. All other versions require upgrading to a release containing the fix (as listed above).

Note: Installing/uninstalling the SWIX will cause the PTP agent to restart.

Version: 1.0

URL:SecurityAdvisory76_CVE-2021-28510_Hotfix.swix

SWIX hash:

```
(SHA-512)2b78b8274b7c73083775b0327e13819c655db07e22b80038bb3843002c679
a798b53a4638c549a86183e01a835377bf262d27e60020a39516a5d215e2fadb437
```

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

Contact information needed to open a new service request may be found at:
https://www.arista.com/en/support/customer-support