Date: May 20th, 2022

Revision	Date	Changes
1.6	May 20th, 2022	Update CVEs affected release info
1.5	January 4th, 2022	Add information about CVE-2021-44832
1.4	December 21st, 2021	Add information about CVE-2021-45105
1.3	December 17th, 2021	Add information about CVE-2021-4104
1.2	December 16th, 2021	Add patch link and more vulnerability details
1.1	December 13th, 2021	Update on affected products and versions
1.0	December 12th, 2021	Initial release

Description

Arista Networks is providing this security update in response to the following related security vulnerabilities:

- CVE-2021-44228 is a Remote Code Execution vulnerability in Apache Log4j2 utility (versions <=2.14.1). An attacker who can control log messages or log message parameters can bypass authentication and execute arbitrary code loaded from malicious LDAP servers when message lookup substitution is enabled.
- CVE-2021-45046 addresses an incomplete fix in Log4j version 2.15.0.
- CVE-2021-4104 is a Remote Code Execution vulnerability by JMSAppender in Log4j version 1.x in non-default configurations.
- CVE-2021-45105 is a Denial-of-Service vulnerability by uncontrolled recursion from self-referential lookups in Log4j2 in a non-default Pattern Layout with a Context Lookup.
- CVE-2021-44832 is a Remote Code Execution vulnerability when a configuration uses a JDBC Appender with a JNDI LDAP data source URI when an attacker has control of the target LDAP server.

Out of all the vulnerabilities, only CVE-2021-44228 and CVE-2021-4104 affect some of Arista's products as listed below.

Arista Engineering and Security teams have deployed fixes to all affected cloud services and are actively developing patches to remaining affected products, and will continue to update this advisory when more information is available.

Vulnerability Assessment

The following products are affected by CVE-2021-44228:

- CloudVision Portal
  - 2019.1.0 to 2021.2.1 (*)
- CloudVision Wi-Fi, virtual appliance or physical appliance
  - 8.8 to 11.0.1 (*)
- Analytics Node
  - 7.0.0 to 8.0.2 (*)
  - Applies to deployments with
    - DANZ Monitoring Fabric (formerly Big Monitoring Fabric)
    - Converged Cloud Fabric (formerly Big Cloud Fabric)
    - Standalone
- Embedded Fabric Analytics module for Converged Cloud Fabric (formerly Big Cloud Fabric)
  - CCF / BCF 5.3.0 to 5.3.8 (*)

(*) The affected products use Log4j 2.x indirectly through Elasticsearch and/or Logstash and are vulnerable to CVE-2021-44228. Based on Arista's analysis of the use of these modules and information provided by Elastic, we believe there is no vulnerability of Remote Code Execution. There is a possibility of Information Leak and/or Denial-of-Service and we recommend the mitigations be implemented.

The following products are affected by CVE-2021-4104:

- Embedded Fabric Analytics module for Converged Cloud Fabric (formerly Big Cloud Fabric)
  - CCF / BCF earlier than 5.3.0

The following cloud services were affected and patches have been deployed:

- CloudVision as-a-Service
- CloudVision Wi-Fi cloud service delivery

The following products are <u>NOT</u> affected:

- Arista EOS-based products
- CloudVision physical appliance
- Arista 7130 Systems running MOS
- Awake Security Platform
- Arista Wireless Access Points
- Other Components of Converged Cloud Fabric and DANZ Monitoring Fabric
  - DMF: Controller, Service Node, Recorder Node
  - Switchlight OS
- Multi-Cloud Director

Patches and Mitigation Instructions

The following document describes detailed steps to patch and mitigate all vulnerabilities on affected products (login required).

References

- https://nvd.nist.gov/vuln/detail/CVE-2021-44228
- https://nvd.nist.gov/vuln/detail/CVE-2021-45046
- https://nvd.nist.gov/vuln/detail/CVE-2021-4104
- https://nvd.nist.gov/vuln/detail/CVE-2021-45105
- https://nvd.nist.gov/vuln/detail/CVE-2021-44832
- https://logging.apache.org/log4j/2.x/security.html
- https://discuss.elastic.co/t/apache-log4j2-remote-code-execution-rce-vulnerability-cve-2021-44228-esa-2021-31/291476

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:

Please visit Customer Support for up to date information on how to open a service request via email or telephone.