Date: November 1, 2022

Revision	Date	Changes
1.0	Nov 1, 2022	Initial release

Description

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

CVE-2022-3602 - An attacker can craft a malicious email address to overflow four attacker-controlled bytes on the stack. This buffer overflow could result in a crash (causing a denial of service) or potentially remote code execution depending on stack layout for any given platform/compiler.

CVE-2022-3786 - An attacker can craft a malicious email address to overflow an arbitrary number of bytes containing the `.` character (decimal 46) on the stack. This buffer overflow could result in a crash (causing a denial of service).

On Tuesday, November 1st it was announced that OpenSSL versions from 3.0.0 to 3.0.6 are vulnerable to two high severity vulnerabilities that if exploited, could result in significant disclosure of sensitive information from memory, remote compromise of system private keys, and potentially remote code execution.

Vulnerability Assessment

No Arista products are affected. Individual products are listed below.

OpenSSL provides multiple release trains which implement cryptography functionality. Arista products use release trains which predate the v3.0 train.

The following products are NOT affected:

- Arista EOS-based products
- Arista Wireless Access Points
- CloudVision Portal, virtual appliance or physical appliance
- CloudVision as-a-Service
- CloudVision Wi-Fi, virtual appliance or physical appliance
- CloudVision Wi-Fi cloud service delivery
- Arista Converged Cloud Fabric and DANZ Monitoring Fabric (Formerly Big Switch Nodes for BCF and BMF)
- Arista 7130 Systems running MOS
- Awake Security Platform
- Untangle NG Firewall and Micro Edge
- Pluribus Netvisor Software

Copyright 2026 Arista Networks, Inc. The information contained herein is subject to change without notice. Arista, the Arista logo and EOS are trademarks of Arista Networks. Other product or service names may be trademarks or service marks of others.

Based upon the foregoing, we believe that the risk of exposure to Arista's systems or products to the OpenSSL issue is low. However, we take threats of cyberattacks on our systems and products very seriously and will continue to monitor the situation.

References

- https://www.openssl.org/news/secadv/20221101.txt

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

Copyright 2026 Arista Networks, Inc. The information contained herein is subject to change without notice. Arista, the Arista logo and EOS are trademarks of Arista Networks. Other product or service names may be trademarks or service marks of others.