Date: May 24, 2024

Revision	Date	Changes
1.0	May 24, 2024	Initial release

The CVE-ID tracking this issue: CVE-2023-52424
CVSSv3.1 Base Score: Not indicated by NVD as of 5/23/2024

Description

Arista Networks is providing this security update in response to the following publicly disclosed security vulnerabilities related to protocol level issues with the 802.11 standard. The IEEE 802.11 standard sometimes enables an adversary to trick a victim into connecting to an unintended or untrusted network with WEP, WPA3 SAE-loop, Enterprise 802.1X/EAP, Mesh AMPE, or FILS. This has been characterized as an "SSID Confusion" issue. This occurs because the SSID is not always used to derive the pairwise master key or session keys, and because there is not a protected exchange of an SSID during a 4-way handshake.

Research papers exposing the vulnerability details :
https://www.top10vpn.com/assets/2024/05/Top10VPN-x-Vanhoef-SSID-Confusion.pdf
https://www.top10vpn.com/research/wifi-vulnerability-ssid/

This issue was reported externally. Arista is not aware of any malicious uses of this issue in customer networks.

Arista Mesh links are not impacted as they use WPA-PSK.

Vulnerability Assessment

Affected Software

Access Point Versions

- All current and unsupported versions of the software

Affected Platforms

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

- All Arista Wireless Access Points

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

- Arista EOS-based products:
  - 710 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/R3 Series
  - 7300X/X3 Series
  - 7320X Series
  - 7358X4 Series
  - 7368X4 Series
  - 7388X5 Series
  - 7500E/R/R2/R3 Series
  - 7800R3 Series
  - CloudEOS
  - cEOS-lab
  - vEOS-lab
  - AWE 5000 Series
- CloudVision CUE, virtual appliance or physical appliance
- CloudVision CUE 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)

- Arista NetVisor OS, Arista NetVisor UNUM, and Insight Analytics (Formerly Pluribus)

Required Configuration for Exploitation

The setup for CVE-2023-52424 involves causing a victim to connect to a Wrong Network when they attempt to connect to a Trusted Network. There is no requirement for the victim to have had any prior connections to the Wrong Network nor to have the Wrong Network stored in their list of known networks.

It is not required that the attacker knows the victim’s authentication credentials, just that the same credentials are used for connecting to both the Wrong and Trusted Networks.

Indicators of Compromise

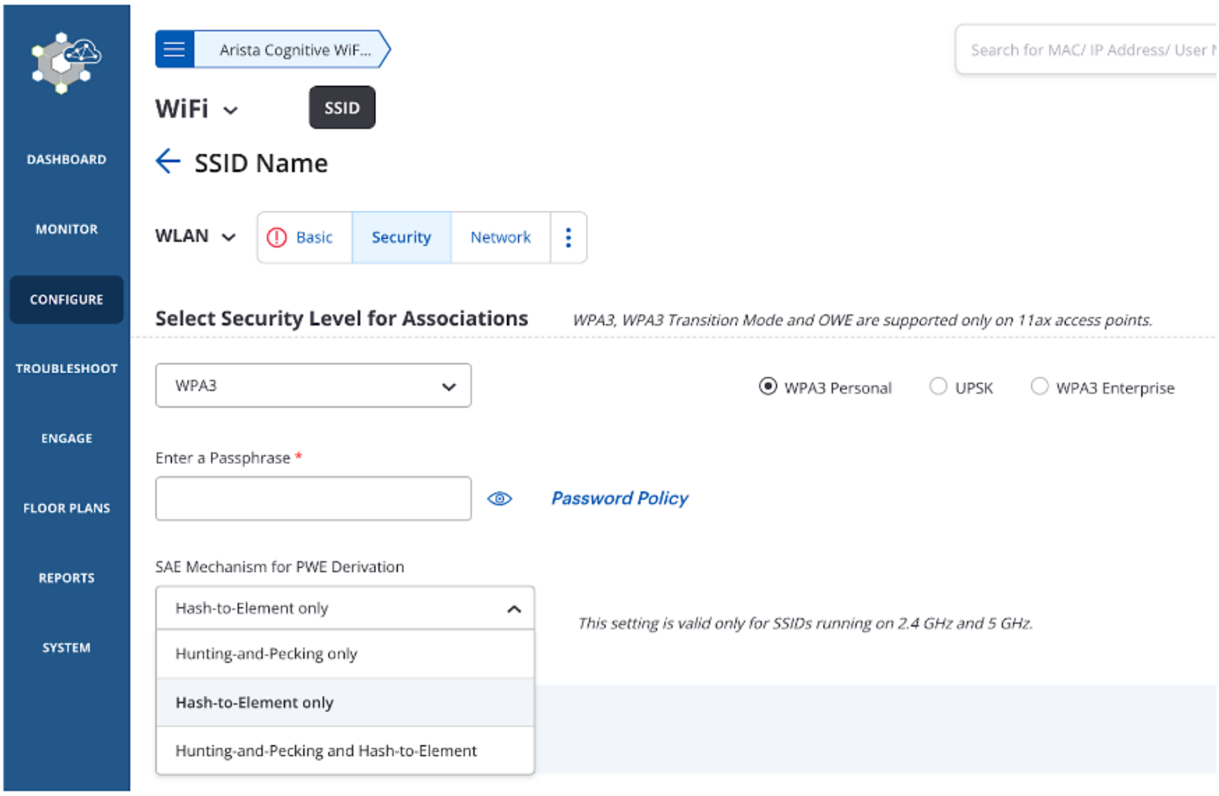
The attacker uses the MAC address (BSSID) of the Wrong network to clone the Trusted network. Due to this the attackers MitM device is detected as a honeypot of the Trusted network by the security monitoring functionality of the Arista APs.

Mitigation

The following steps will mitigate the attack:

1. Avoid using the same RADIUS credentials across different SSIDs.

2. Avoid using WPA3 SAE with Hunting & Pecking, and use WPA3 SAE with Hash to Element instead
   Configure -> WiFi -> Select SSID for Edit -> Security



Select Security Level for Associations

WPA3, WPA3 Transition Mode and OWE are supported only on 11ax access points.

WPA3

● WPA3 Personal ○ UPSK ○ WPA3 Enterprise

Enter a Passphrase *

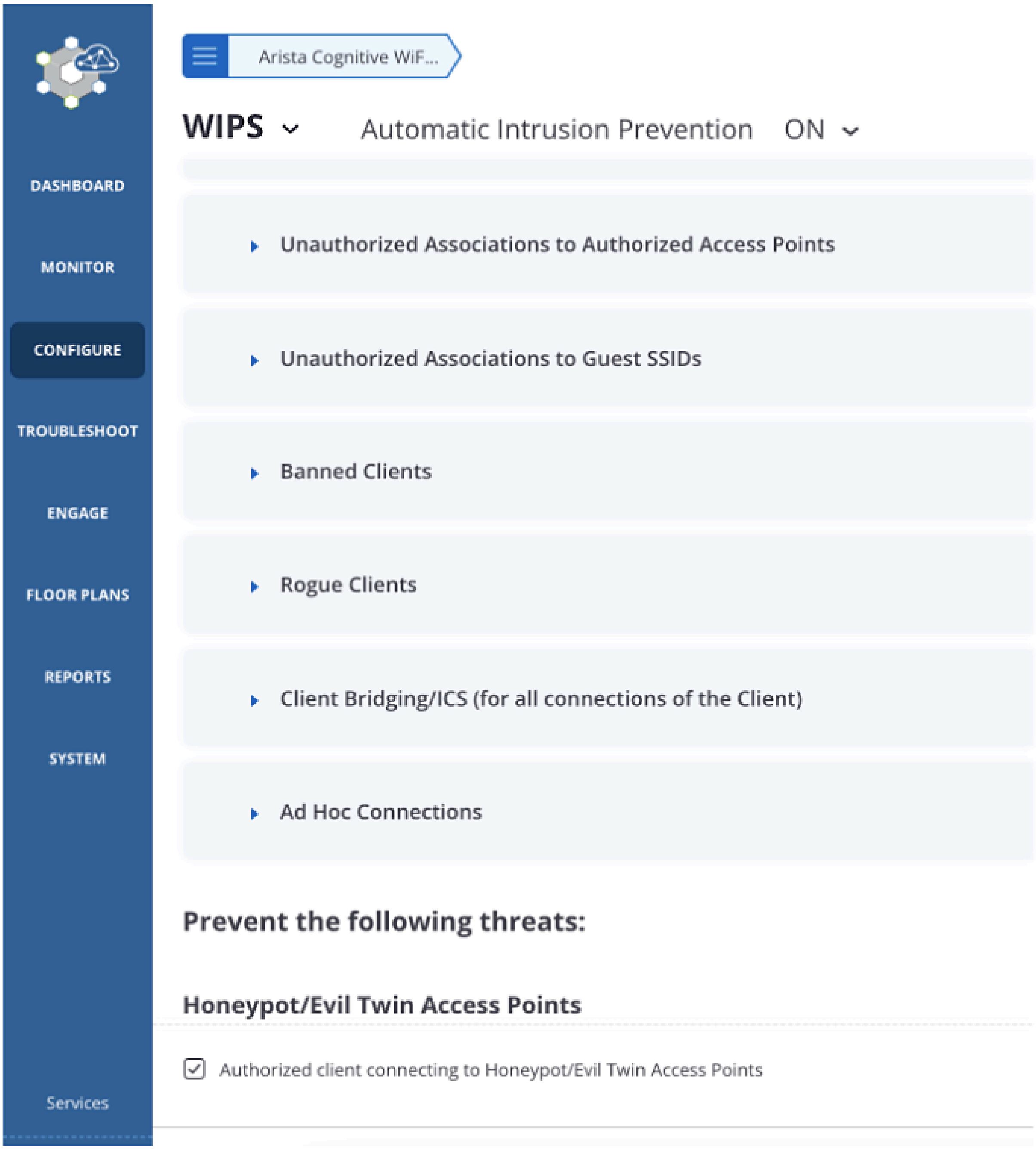
SAE Mechanism for PWE Derivation

Hash-to-Element only

- Hunting-and-Pecking only
- Hash-to-Element only
- Hunting-and-Pecking and Hash-to-Element

This setting is valid only for SSIDs running on 2.4 GHz and 5 GHz.

3. Enable HoneyPot/Evil Twin prevention to block the client from connecting to the MitM device.
   Configure -> WIPS -> Automatic Intrusion Prevention -> Turn ON
   Configure -> WIPS -> Automatic Intrusion Prevention -> Enable Authorised Client connecting to Honeypot/Evil Twin Access Point.



WIPS ⌄ Automatic Intrusion Prevention ON ⌄

▸ Unauthorized Associations to Authorized Access Points

▸ Unauthorized Associations to Guest SSIDs

▸ Banned Clients

▸ Rogue Clients

▸ Client Bridging/ICS (for all connections of the Client)

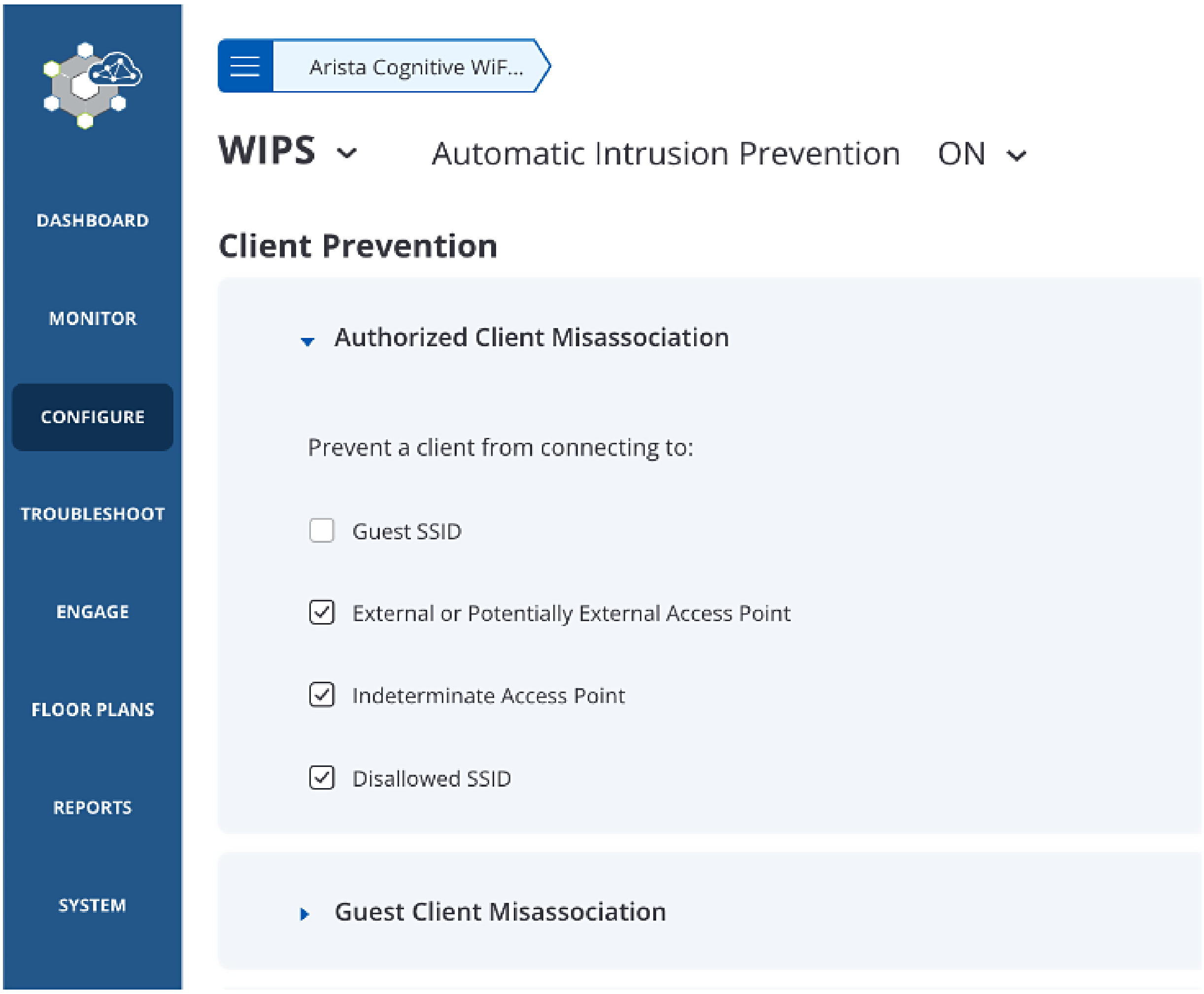
▸ Ad Hoc Connections

Prevent the following threats:

Honeypot/Evil Twin Access Points

☑ Authorized client connecting to Honeypot/Evil Twin Access Points

4. Enable prevention policy that disallows authorized client connection to unauthorized APs.
   (This does not work with Management Frame Protection enabled)



WIPS Automatic Intrusion Prevention ON

Client Prevention

Authorized Client Misassociation

Prevent a client from connecting to:

- □ Guest SSID
- ☑ External or Potentially External Access Point
- ☑ Indeterminate Access Point
- ☑ Disallowed SSID

Guest Client Misassociation

5. Disable the Auto VPN feature to avoid disabling VPN on trusted networks. VPN should be active in home/hotspot areas.

Resolution

Because this is a protocol level issue requiring changes to the IEEE 802.11 standard no patches or software updates apply.

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