aruba

a Hewlett Packard Enterprise company

IDS Feature for WPA2 Attack Detection

October 16, 2017

WPA2 Vulnerability

- Related to WPA2 key handshakes
- Attacker does key reinstallation attack via retransmitting message 3 of WPA2 4 way key handshakes
- When 802.11r is enabled, the attacker does key reinstallation attack against FT (Fast BSS Transition) handshake via retransmitting reassociation requests

Releases for WPA2 Attack Detection Feature

- ArubaOS 6.3.1.25
- ArubaOS 6.4.4.16
- ArubaOS 6.5.1.9
- ArubaOS 6.5.3.3
- ArubaOS 6.5.4.2
- ArubaOS 8.2.0.0

IDS Configuration for WPA FT Attack & MitM Detection

- Enable WPA FT attack detection (By default: disabled)
- Enable channel based man in the middle attack detection (By default: disabled)
- Enable AP spoofing detection (By default: enabled)
- Enable ids logging (By default: disabled)

IDS DOS Profile

```
(config) #ids dos-profile default
(IDS Denial Of Service Profile "default") #detect-wpa-ft-attack
```

IDS Impersonation Profile

```
(config) #ids impersonation-profile default
(IDS Impersonation Profile "default") #detect-chan-based-mitm
(IDS Impersonation Profile "default") #detect-ap-spoofing
```

Security Log

```
(config) #logging security subcat ids level warnings
```

SNMP Trap

SNMP Trap for MitM attack
#show snmp trap-queue | include Spoofed 2017-10-06 11:07:00 An AP (NAME AP225 and MAC 18:64:72:cc:0a:e2 on RADIO 1) detected a possible channel-based Man in the Middle attack. Spoofed beacon frame has source address of 18:64:72:40:ae:30, a BSSID of 18:64:72:40:ae:30, announcing a channel switch to CHANNEL 149. SNR is 53. 2017-10-06 11:07:00 An AP (NAME AP225 and MAC 18:64:72:cc:0a:e2 on RADIO 1) detected a frame that has a spoofed source address of 18:64:72:40:ae:30, a BSSID of 18:64:72:40:ae:30, a destination address of ff:ff:ff:ff:ff:ff, and is on CHANNEL 36. SNR is 53, and FrameType is Beacon.

SNMP Trap for WPA2 FT attack
#show snmp trap-queue | include Transition 2017-10-05 09:39:46 An AP (NAME AP225 and MAC 18:64:72:cc:0a:e2 on RADIO 2) detected a possible attack of the Fast BSS Transition for CLIENT 00:22:5f:8c:b4:cf on BSSID 18:64:72:40:ae:20 and CHANNEL 1. 2017-10-05 09:39:46 An AP (NAME correlated-AP225 and MAC 18:64:72:cc:0a:e2 on RADIO 2) detected a possible attack of the Fast BSS Transition for CLIENT 00:22:5f:8c:b4:cf on BSSID 18:64:72:40:ae:20 and CHANNEL 1.

Security Log

Security Log for Man in the Middle Attack:

#show log security all | include Spoofed
Oct 5 09:51:04 :126116: <3840> <WARN> |wms| |ids| AP(18:64:72:40:ae:30@AP225): Man in the Middle Attack: An AP detected a possible channel-based Man in the Middle attack. Spoofed beacon frame has source address of 18:64:72:40:ae:30, a BSSID of 18:64:72:40:ae:30, announcing a channel switch to CHANNEL 149. SNR is 65. Additional Info: SSID:Test-wpa2; Cur-Chan:36; CSA-Chan:149.

Oct 5 09:51:04 :126069: <3840> <WARN> |wms| |ids| AP(18:64:72:40:ae:30@AP225): AP Spoofing: An AP detected a frame that has a spoofed source address of 18:64:72:40:ae:30, a BSSID of 18:64:72:40:ae:30, a destination address of ff:ff:ff:ff:ff:ff, and is on CHANNEL 36. SNR is 65, and FrameType is Beacon. Additional Info: SSID:Test-wpa2. Associated WVE ID(s): WVE-2005-0019.

Security Log for FT Attack:

#show log security all | include Transition
Oct 6 10:57:56 :126115: <4086> <WARN> |wms| |ids| AP(6c:f3:7f:e7:45:e0@AP225-2): WPA FT Attack: An AP detected a possible attack of the Fast BSS Transition for CLIENT 00:22:5f:8c:b4:cf on BSSID 6c:f3:7f:e7:45:e0 and CHANNEL 1. Additional Info: Avg-PktRate(pps):0.8; Interval(sec):60; Channel:1; BSSID:6c:f3:7f:e7:45:e0.

WMS Events Counters

WMS Counter

#show wms counters events

Related Event Configuration

Name	Value
wms-on-master	enable
event-correlation	logs-and-traps
event-correlation-quiet-time	900

Event Counters

ID	Name	Rx-AP	Rx-WMS	DB Updated	DB Inserted	DB Deleted	Corr EvGen	Corr EvSupp
3	Interfering AP	42	14	0	0	0	0	0
77	AP Spoofing	1	0	1	0	0	1	0
120	WPA FT Attack	4	0	4	0	0	2	2
121	Man in the Middle Attack	1	0	1	0	0	1	0

RF Protect License

- RF protect license is required to enable WPA FT attack detection and Channel based Man-in-the-Middle attack.