FREQUENTLY ASKED QUESTIONS

WPA SECURITY VULNERABILITY

V1.1 - OCTOBER 16, 2017

Q: What happened?

A: A researcher has published a paper documenting fairly widespread vulnerabilities in various implementations of WPA2. The vulnerabilities are related to different key handshakes, used between the Wi-Fi supplicant (client) and the AP (authenticator) to derive and install encryption keys. Different implementations respond in different ways when keying handshake messages are retransmitted – some of these responses did not anticipate that the retransmission may be due to an attacker's action rather than simple packet loss. Because these vulnerabilities are related to implementation flaws, they can be fixed through software updates.

One vulnerability is related to 802.11r (also known as Fast BSS Transition). This vulnerability is in the protocol itself, where the protocol does not adequately protect against malicious attack. It is possible to mitigate this vulnerability through a software update as well.

Q: What is the impact?

A: When used successfully against WPA2 with AES-CCMP (the default mode of operation for most Wi-Fi networks), an attacker can decrypt and replay Wi-Fi frames, but cannot forge packets and inject them into the network. When used against WPA-TKIP – an encryption scheme that already suffers from serious security weaknesses and is not recommended for use – an attacker can decrypt, replay, and forge Wi-Fi frames.

Exactly *which* frames can be decrypted, replayed, and (possibly) forged is slightly more complicated. Table 3 of the research paper provides the answer. If a vulnerable client is attacked through the 4-way handshake vulnerability, only client-to-AP traffic can be attacked. If a vulnerable AP is attacked through the 802.11r FT handshake, then AP-to-client traffic can be attacked. Disabling 802.11r on the AP (or installing software updates to fix the vulnerability) will block the ability to attack AP-to-client traffic.

Q: What makes this attack possible?

A: Wi-Fi uses AES-CTR (Advanced Encryption Standard in Counter Mode) to provide confidentiality. With AES-CTR, the combination of a specific key and nonce value should only be used once to encrypt a block of plaintext. If the combination is used twice, an attacker can possibly decrypt the two pieces of plaintext – particularly if the plaintext contains easily predicted values such as IP packet headers. The attack described in the paper does exactly this – it causes various implementations of WPA2 to re-use the same key/nonce multiple times.

Q: Is the attack difficult to carry out?

A: An attacker must establish a man-in-the-middle position between a client and an AP. Further, the AP must be impersonating the MAC address of a legitimate AP, and must be on a different channel. There are existing tools that can create such a scenario. Someone will then need to write code to attack the newly exposed vulnerability. Finally, tools will be needed to perform decryption of traffic based on a reused nonce/key combination. Aruba's assessment is that this is within the capabilities of a skilled attacker with cryptography and Wi-Fi experience, but it will likely take some time before easy-to-use tools are developed.

Q: Why are so many vendors affected by this?

A: The IEEE 802.11 specification was silent about how to handle certain conditions, so that an implementation could be 100% standard-compliant but still vulnerable. In particular, the standard told implementers *what* to do, but not necessarily *when* to do it. To protect against this vulnerability, implementers must add additional state machine checks beyond what the standard requires. All vendors worked from the same specification documents, which is why the flaw is widespread.

Q: Does this affect WPA2-PSK or WPA2-Enterprise?

A: Both are affected. The attack is against the key exchange handshake, not against the authentication exchange.

Q: Does this affect Wi-Fi infrastructure (APs/controllers), Wi-Fi clients, or both?

A: Both are affected.

Q: Does this mean WPA2 is broken now?

A: No. The vulnerability is due to implementation flaws (programmers did not anticipate and guard against a particular set of circumstances when writing the code) rather than a protocol-level weakness. Contributing to the problem was insufficient/ambiguous guidance to developers in the 802.11 standard. All vulnerabilities can be mitigated through software updates to affected systems without the need for a change in the protocol.

Q: Will there be additional vulnerabilities exposed in the future?

A: All currently known vulnerabilities have been made public at this time. We expect that as a result of this set of vulnerabilities, additional research will be performed, both by private researchers and by the IEEE 802.11 committee. It is possible that additional vulnerabilities may be uncovered in the future.

Q: Does the attack expose my credentials or keys?

A: The attack does not expose WPA2 authentication credentials such as passwords or pre-shared keys. There is no need to change passwords or re-key a Wi-Fi network in the wake of this vulnerability.

Q: How are Aruba controlled APs and Mobility Controllers running ArubaOS affected?

A: ArubaOS contains both *authenticator* and *supplicant* functionality. The two are affected differently:

- As an *authenticator* (standard WPA2 functionality where the AP/controller exchanges encrypted information with a Wi-Fi client), ArubaOS is **not vulnerable** to the key reinstallation attack in the 4-way and group key handshakes. This is because ArubaOS stores the latest value of the replay counter and will reject any message that contains a different replay value.
- As an *authenticator* in the 802.11r Fast BSS Transition (FT) handshake, ArubaOS is **vulnerable** to the key reinstallation attack. This is made possible because the first two messages of the FT handshake do not contain a replay counter. Aruba has mitigated this attack through a software update. Note that 802.11r is *not enabled* by default in ArubaOS; the majority of Aruba customers will not be affected. For customers who have enabled 802.11r, disabling it will prevent the attack. *Bug 168097 is tracking this issue.*
- The “mesh” feature of ArubaOS allows APs to connect to other APs over wireless links for the purpose of network extension. Mesh links are protected using WPA2, and the open-source Linux “wpa_supplicant” utility is used to provide 802.1X authentication. The research paper points out that wpa_supplicant is vulnerable to the key reinstallation attack. Mesh is *not enabled* by default in ArubaOS. For customers who have enabled this feature, disabling it will prevent the attack. *Bug 168489 is tracking this issue.*

Q: Do I need to upgrade ArubaOS?
A: Upgrading your ArubaOS software is recommended to fully mitigate all vulnerabilities.

Q: Which versions of ArubaOS software contain the fixes?
A: The vulnerabilities have been fixed in the following ArubaOS patch releases, which are all available for download immediately:

- 6.3.1.25
- 6.4.4.16
- 6.5.1.9
- 6.5.3.3
- 6.5.4.2
- 8.1.0.4

Q: The release notes for those versions doesn't say anything about fixing vulnerabilities. Are they really fixed in those versions?
A: Software updates were published prior to the vulnerabilities becoming public. As a standard practice, Aruba does not add vulnerability information into release notes until after a vulnerability has become public. The release notes will be revised now and re-posted.

Q: What about ArubaOS 5.x, 6.1, 6.2, and 6.5.2.x?
A: ArubaOS 5.x reached its end-of-support date in May 2016 and is no longer supported or maintained. Aruba 6.1 and 6.2 reached their end-of-support date in May 2015. See http://www.arubanetworks.com/support-services/end-of-life/ for more information.

ArubaOS 6.5.2.x was a "controlled release" with different support policies than standard. The differences between 6.5.3.x and 6.5.2.x were relatively minor at the time that 6.5.3 was introduced. Since that time, 6.5.2.x has not been maintained. Customers can migrate to 6.5.3.x with minimal risk.

Q: How is Aruba Instant affected?
A: InstantOS contains both *authenticator* and *supplicant* functionality. The two are affected differently:

- As an *authenticator* (standard WPA2 functionality where the AP exchanges encrypted information with a Wi-Fi client), InstantOS is **not vulnerable** to the key reinstallation attack in the 4-way and group key handshakes. This is because InstantOS stores the latest value of the replay counter and will reject any message that contains a different replay value.
- As an *authenticator* in the 802.11r Fast BSS Transition (FT) handshake, InstantOS is **vulnerable** to the key reinstallation attack. This is made possible because the first two messages of the FT handshake do not contain a replay counter. Aruba has mitigated this attack through a software update. Note that 802.11r is *not enabled* by default in InstantOS; the majority of Aruba customers will not be affected. For customers who have enabled 802.11r, disabling it will prevent the attack. *Bug 168101 is tracking this issue.*
- The "mesh" feature of InstantOS allows APs to connect to other APs over wireless links for the purpose of network extension. Mesh links are protected using WPA2, and the open-source Linux "wpa_supplicant" utility is used to provide 802.1X authentication. The research paper points out that wpa_supplicant is vulnerable to the key reinstallation attack. Mesh is *not enabled* by default in InstantOS 4.1 and higher – in previous versions of InstantOS, mesh was enabled by default. For

customers who have enabled this feature, disabling it will prevent the attack. *Bug 168100 is tracking this issue.*

- IAP contains a feature called "Wi-Fi Uplink", which allows an IAP to connect as a Wi-Fi client to another AP. This feature uses the open-source "wpa_supplicant" utility to provide 802.1X authentication, and is vulnerable to the key reinstallation attack. Wi-Fi Uplink is *not enabled* by default in InstantOS. For customers who have enabled this feature, disabling it will prevent the attack. *Bug 168100 is tracking this issue.*

Q: Do I need to upgrade InstantOS?
A: Upgrading your InstantOS software is recommended to fully mitigate all vulnerabilities.

Q: Which versions of InstantOS software contain the fixes?
A: The vulnerabilities have been fixed in the following InstantOS patch releases, which are all available for download immediately:

- 4.2.4.9
- 4.3.1.6
- 6.5.3.3
- 6.5.4.2

Q: The release notes for those versions doesn't say anything about fixing vulnerabilities. Are they really fixed in those versions?
A: Software updates were published prior to the vulnerabilities becoming public. As a standard practice, Aruba does not add vulnerability information into release notes until after a vulnerability has become public. The release notes will be revised now and re-posted.

Q: I don't have a support contract with Aruba. Can I still download new software?
A: In this circumstance, Aruba will provide software updates to anyone who requests it, regardless of support contract status. Contact Aruba Support through one of the phone numbers listed at http://www.arubanetworks.com/support-services/contact-support/.

Q: How is Clarity Synthetic / Clarity Engine affected?
A: Some customers have been beta-testing a new feature called "Clarity Synthetic," which allows an Aruba access point to act like a Wi-Fi client, connecting and authenticating to another Aruba AP for the purpose of testing network performance. Clarity Synthetic is not an ArubaOS feature in its current form – it is a separate system. Clarity Engine contains the open-source Linux "wpa_supplicant" utility to provide 802.1X authentication. The research paper points out that wpa_supplicant is vulnerable to the key reinstallation attack. Customers participating in the Clarity Synthetic beta should not use the feature until they update the software. Clarity Engine 1.0.0.1 contains a fix for the vulnerability.

Clarity Synthetic differs from "Clarity Live" – the latter is an ArubaOS feature that uses only passive monitoring of wireless traffic to create performance statistics. Clarity Live is not affected by the key reinstallation vulnerability.

Q: How is the Aruba 501 Client Bridge affected?
A: The client bridge acts as a Wi-Fi supplicant and incorporates the open-source wpa_supplicant code. It is vulnerable in a similar way to other Aruba products that contain supplicant functionality. Updated

software is available for this product to address the issue and may be downloaded from the HPE My Networking Portal site.

Q: How are other Hewlett Packard Enterprise (HPE) wireless products affected?

A: Aruba has reached out to the teams responsible for the HP MSM series of controllers and the HPE 8xx Unified WLAN Appliance series to obtain status. A separate security advisory will be issued (https://www.hpe.com/us/en/services/security-vulnerability.html) with full details. It has been reported that these products are **not vulnerable** to the key reinstallation attack in the 4-way handshake or group key handshake when acting as an 802.1X authenticator. The products do not support 802.11r and are **not vulnerable** to the FT handshake vulnerability.

Q: What exactly did Aruba change in the new software?

A: Most of the Aruba-specific vulnerabilities came from use of the open-source *wpa_supplicant* software to provide Wi-Fi client functionality for certain features. Aruba, through cooperation with the author of wpa_supplicant and ICASI, was provided with patches to this software that address the vulnerabilities. Additionally, Aruba addressed the FT handshake vulnerability by ensuring that a given nonce/PTK combination can only be used once; if a key must be reinstalled, a new nonce will be created.

Q: Will the fixes lead to any interoperability problems? What about performance degradation?

A: The fixes should not result in interoperability issues. The Wi-Fi Alliance has added specific tests related to these vulnerabilities to its interoperability test suite and has made its lab available to member companies for the purpose of verifying continued interoperability after fixes are made. Aruba is participating in this program. The fixes also should not result in any performance degradation or delays during roaming.

Q: I can't upgrade my software immediately. Are there workarounds?

A: Yes. See the explanation above for either ArubaOS or InstantOS to determine workarounds. Disabling vulnerable features will effectively mitigate these attacks.

Q: The workarounds aren't practical for me. What is my risk if I don't upgrade?

A: Risk will depend on individual circumstances. For example, if all critical enterprise data is protected in transit using HTTPS/TLS in addition to WPA2, then a partial loss of WPA2 security may not be viewed as critical. In general, Aruba believes this is an *important* update, but not an *emergency* update. It will take time before attack tools become widely available. Once tools do become available, the risk of decryption and replay appears to be limited to uni-directional traffic from the client to the AP.

Q: The research paper mentions that it is easier to attack the group key handshake on clients if the AP immediately installs a new group key. What does Aruba do?

A: Aruba immediately installs the group key after sending Group Message 1, and does not wait until all stations reply with Group Message 2. Aruba found through trial and error that waiting for all stations to respond led to network instability in enterprise networks. The problem in enterprise networks is that typically an AP is dealing with a large number of clients. Clients may go into power-save mode, may go to sleep, may roam out of Wi-Fi coverage, or disappear for a number of other reasons. If the AP waits for all stations to acknowledge a group key message, it may be left waiting forever – leaving the AP and stations unable to send broadcast and multicast traffic in the interim. Therefore, the decision was made to immediately install and begin using the new group key. Unfortunately, this behavior does make attacking the group key easier when using an unpatched client device.

Q: If I upgrade my Aruba software, does that solve the entire problem?

A: Not necessarily. Aruba is providing only the infrastructure side of a Wi-Fi network. The client side must also be considered. You will need to determine if you are using vulnerable client devices, such as laptops, tablets, phones, and IoT devices, in your network. All major vendors of Wi-Fi client devices have been notified of this vulnerability, and most should have impact statements and further information available.

In addition, it is possible that new information will become available that will necessitate additional software updates. If Aruba learns of additional vulnerabilities, that information will be communicated through Aruba's standard vulnerability disclosure process.

Q: This means I need to update both the infrastructure AND the clients to be fully protected?

A: Correct. Updating just one half of the solution does not effectively solve the problem. However, an effective mitigation would be disabling 802.11r on the Aruba infrastructure while updating clients that are vulnerable to the 4-way handshake vulnerability.

Q: If I disable 802.11r on the AP/controller, are the clients still vulnerable to the FT handshake issue?

A: If 802.11r is not enabled on the infrastructure, clients would not attempt to reassociate using the FT handshake. An attacker would not be able to exploit the FT handshake vulnerability in this situation.

Q: Can I detect if someone is attacking my network or devices?

A: Aruba software checks for replay counter mismatches on a per-client basis and will produce a log message if detection is triggered. The log message begins with "`Replay Counter Mismatches`", followed by additional details.
Aruba has also released new RFProtect (WIDS) features and signatures to help detect attacks. These features are available in the following ArubaOS releases:

- 6.4.4.16
- 6.5.1.9
- 6.5.3.3
- 6.5.4.2
- 8.2.0.0

Q: When did Aruba find out about this?

A: Aruba was notified by the author of the research paper on July 15, 2017, and by the CERT Coordination Center on August 28, 2017. Aruba was also contacted by ICASI on September 12, 2017. Aruba signed an NDA with ICASI in order to further participate in industry-level discussions.

Q: Why is Aruba disclosing this now?

A: A vulnerability of this scale requires coordination between multiple vendors and other interested parties so that responses and patches may be prepared in advance of the vulnerability becoming widely known. The vendor community (represented by ICASI), in cooperation with the author, CERT, and the Wi-Fi Alliance jointly agreed on October 16 as the disclosure date for this vulnerability.

Q: Did Aruba provide advance notification to any customers or partners?

A: No. Aruba does not engage in selective vulnerability disclosure.

Q: How many other vendors are affected?

A: It appears that all vendors of Wi-Fi equipment and clients are affected to at least some extent.

.

Q: Where can I read all the details about the vulnerability and attack?

A: The original research paper is entitled "Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2" by Mathy Vanhoef and was submitted to the 24th Association for Computing Machinery (ACM) Conference on Computer and Communications Security. It may be downloaded from: https://papers.mathyvanhoef.com/ccs2017.pdf.

Q: Where can I ask questions?

A: Visit https://community.arubanetworks.com where active discussion forums exist. These forums will be monitored throughout the coming weeks.

.

Q: Does the 802.11r FT handshake vulnerability also apply to OKC?

A: Opportunistic key caching (OKC) is a non-standard but widely-implemented method for achieving fast roaming. It existed before the creation of 802.11r. OKC does not use the FT handshake and is not affected by the FT handshake vulnerability.

Q: Some people are saying this is a protocol flaw, and some people are saying it's an implementation flaw. Which is it?

A: It is both. However, the *fix* is in the implementation; we do not require a new protocol. Specifically:

- The 802.11r FT handshake vulnerability is a protocol-level flaw. The protocol was not designed to resist this attack. Vendors can retroactively patch the flaw, however, in a way that does not affect interoperability. This is what Aruba and other vendors have done.
- The 4-way handshake, group handshake, and other keying vulnerabilities result from the 802.11i standard (the description and specification of the protocol) being insufficiently detailed. That has been compounded by certain Android/Linux implementations that make the flaw worse than it otherwise would have been. Vendors can add logic to patch the flaw.