Aruba Support Advisory ARUBA-SA-20191219-PLVL08

Aruba Instant Certificate Expiry Issue

Confidentiality Level: Aruba Customers & Partners only | Rev-2 (January 6, 2020)

OVERVIEW

There is a software defect that may impact Aruba Instant Access Points (IAP) and its accessibility through Aruba Central, Activate, and AirWave. This bug is tied to an SSL certificate in the Trust Anchor (TA) file of Instant OS, and may result in the loss of connectivity to management platforms unless the recommended action is taken prior to February 07, 2020. This is not a security vulnerability, but a software defect that may cause loss of connectivity to management plane.

DESCRIPTION OF THE ISSUE

One of the Verisign certificates within the TA certificate bundle will expire on February 07, 2020. Although an updated version of this certificate is included in Instant software, the defect in the SSL library will ignore all valid certificates if a single expired certificate is encountered. The existing IAP deployments will fail to set up an SSL connection to Central, Activate, and AirWave due to this defect.

Please Note: IAPs are designed to operate without these services, and they will remain functional and forward traffic after February 07, 2020. Also, existing Central and AirWave sessions will remain active after February 07, 2020. However, if there is loss of connectivity or a reset of any of the Central or AirWave service, the connectivity between IAP and the management platforms will not remain active and IAP deployments will revert to local management mode, built into the IAP. To re-connect to the management services, a manual upgrade of every IAP cluster and every IAP in standalone mode is required. The upgrade will load a patch that will re-establish connectivity to Central, Activate, or AirWave. Due to the above conditions, all customers with affected IAP deployments are strongly advised to upgrade to a software version with the fix prior to February 07, 2020.

Revision-2 of this advisory as of Jan 06, 2020 includes an update and remediation for - a different defect that affects Instant 8.6.0.0 and 8.6.0.1 deployments managed by AirWave with certificate-based authentication. Please read the entire advisory for relevant details.

AFFECTED PRODUCTS

IAPs that require connectivity to Central, Activate, and/or AirWave may be affected.

- For IAPs managed by Central with connectivity to Activate, following software versions and IAP platforms are affected.

Affected Software Version (Currently Supported Only)	Affected IAP Platforms
All software versions prior to Instant 8.6.0.0 (8.5.x.x, 8.4.x.x, 8.3.x.x, 6.5.x.x, 6.4.x.x-4.2.x.x)	All IAP platforms (IAP-1XX, RAP-XXX, IAP-2XX, IAP-3XX and IAP-5XX series products)
Instant 8.6.0.0	RAP-155, IAP-214, IAP-215, IAP-224, IAP-225, IAP-228, IAP-274, IAP-275, and IAP-277

- For IAPs managed by AirWave with certificate-based authentication, following software versions and IAP platforms are affected. It is estimated that less than 10% of IAPs deployed use this option.

Affected Software Version (Currently Supported Only)	Affected IAP Platforms
All software versions prior to Instant 8.6.0.1 (8.6.0.0, 8.5.x.x, 8.4.x.x, 8.3.x.x, 6.5.x.x, 6.4.x.x-4.2.x.x)	All IAP platforms (IAP-1XX, RAP-XXX, IAP-2XX, IAP-3XX and IAP-5XX series products)
Instant 8.6.0.1	All AP-3XX, and AP-5XX, AP203H/203R/203RP, and IAP-207

For details on the impact to customer deployments using different management options, refer to the section titled **DETAILED CUSTOMER IMPACT DUE TO DEFECT** below.

Note: An Instant deployment running a C-build that meets any one of the above listed conditions is also impacted.

PRODUCTS NOT AFFECTED

Software Version	IAP Platforms
AP platforms running Instant 8.6.0.1	RAP-155, IAP-214, IAP-215, IAP-224, IAP-225, IAP-228, IAP-274, IAP-275, and IAP-277
Controller-based access points (CAP) and Remote access points (RAP)	

CUSTOMER DEPLOYMENTS NOT AFFECTED

This issue does NOT affect the following Instant deployment scenarios with any IAP platforms.

- AirWave managed deployments using PSK-based device authentication
- Instant customers not using Central, AirWave, or Activate, but locally managing Instant clusters
- Customers with deployment of FIPS certified version of IAP
- Future deployments of un-provisioned APs in factory-default state
- If un-provisioned APs in factory-default state are deployed in an environment that offers connection to the internet for the APs to reach Activate, then Activate will be able to force an upgrade to a software version with a fix for the issue over an unsecure channel. The upgraded APs will then come back online, set up a secure connection with Activate, and proceed to the next step that includes redirection to Aruba Central or AirWave successfully.
- If un-provisioned APs in factory-default state are deployed in an environment that offers no connection to Internet for the APs to reach Activate, then Activate will not be able to perform an upgrade of the APs automatically. In such cases, the customer must manually upgrade the APs to a software version with the fix, by either using AirWave with PSK based authentication or using local management option within the master AP of the Instant cluster.
- New controller-based AP deployments
- If Internet connection is available to the APs in a new controller-based deployment, the APs will still reach out to Activate and Activate will force an upgrade of the APs to a software version with the fix. After the upgrade, the APs will connect to the controller.
- If Internet connection is not available, the APs will still be able to connect to the controller.

WHAT HAPPENS IF …

If the affected customer deployments are NOT upgraded by Feb 07, 2020, then,

- IAPs will continue to provide client connectivity and forward traffic as designed. There is no impact to WLAN operation of the Instant cluster.
- Existing connection of IAPs with Central and AirWave will continue to remain as is after February 07, 2020. However, if that connection were to reset due to either a loss of Internet connectivity, a reboot of AirWave, or a reset of Central, the impacted versions of IAP will not be able to reestablish a new SSL connection back to the management platform. This issue only affects connectivity between IAP and management platforms.

RESOLUTION

The certificate expiry error bug is fixed in following software patches of all the supported release versions:

Instant Patch	Release Date
6.4.4.8-4.2.4.16	19-Dec-2019 (Posted)
6.5.4.15	20-Dec-2019 (Posted)
8.3.0.11	21-Dec-2019 (Posted)
8.4.0.6	17-Dec-2019 (Posted)
8.5.0.5	09-Dec-2019 (Posted)
8.6.0.2	07-Jan-2020

Please note the following:

- Instant OS 6.5.x.x-4.3.x.x and 6.5.3.x release versions are at end-of-support. Customers running either of these two software versions are advised to upgrade to Instant OS 6.5.4.15.
- Instant OS 6.4.4.8-4.2.x.x is the last supported release version for RAP-3, RAP-108, RAP-109, IAP-103, IAP-104, IAP-105, IAP-134, IAP135, and IAP-175. Customer deployments with these AP platforms are advised to upgrade to Instant OS 6.4.4.8-4.2.4.16.
- Instant OS 6.5.4.x is the last supported version for IAP-204, IAP-205, IAP-205H, IAP-114, and IAP-115. Customer deployments with these AP platforms are advised to upgrade to Instant OS 6.5.4.15.
- Instant 8.6.x.x is the last supported version for RAP-155, IAP-214, IAP-215, IAP-224, IAP-225, IAP-228, IAP-274, IAP-275, IAP-277. So, customer deployments with these AP platforms are advised to upgrade to Instant 8.6.0.2.
- Customer deployments running c-builds need to upgrade to one of the software patches with the bug fix, as applicable. You may reach out to your Aruba Account team or Aruba Global Support, to review your upgrade options or if you have any questions.

Software upgrade test of an Aruba Central-managed IAP Cluster

- In Aruba's testing, Instant OS upgrade of a (mixed / two-class) 128 IAP cluster, managed through Aruba Central over a 1Mbps (worst-case) internet link, took less than 15 minutes to upgrade all the IAPs.
- With 15 minutes for pre-upgrade inspections and post-upgrade validation, a 128 Instant AP cluster upgrade should be completed in under 30 minutes, on an average.

DETAILED CUSTOMER IMPACT DUE TO DEFECT

Listed below are the management service options that will be impacted by this issue, if the software is not upgraded to the recommended version, before February 07, 2020.

Activate connection

- All IAPs with an Internet connection connect to Activate to get zero-touch provisioning (ZTP) rules. Also, IAPs periodically connect with Activate to synchronize on provisioning rules and software versions available. Without running one of the recommended fixed software versions, IAP will lose connectivity to Activate. Clients continue to be served and traffic within clusters is maintained. Periodic synchronization to Activate will not be available until the cluster is upgraded to a software version with the fix.

Central-managed IAPs

- For Central-managed IAPs, connectivity to Central is lost on connection reset. Clients continue to be served and traffic within clusters is maintained. However, the IAPs become unreachable from Central and they fall back to local management built into the IAPs. Restoring connectivity to Central requires a manual upgrade of the cluster to a software version with the fix.
- An existing connection between IAP and Central may be reset due to several reasons including WAN or Internet connection issues, reboot of the IAP, and Central upgrades that include Context Engine changes.
- If Central connection is reset due to any reason, then Central will lose access to the IAPs. This will impact all Central customers who do not upgrade their affected IAPs to a software version with the fix before February 07, 2020.

AirWave-managed IAPs

- There will be impact on AirWave managed IAP deployments upon reset of existing connection depending on the authentication method selected (certificate-based or PSK-based).
- For customers using certificate-based authentication option between AirWave and IAP, there will be a loss of connection to AirWave when the existing connection is reset.
- For customers using PSK based authentication option between AirWave and IAP, there is no impact.
- An existing connection between IAP and AirWave may reset due to several reasons including LAN or WAN connection issues between IAP and AirWave, reboot of the IAP, reboot of AirWave, and upgrade of AirWave software
- There is a different defect present in Instant 8.6.0.0 and 8.6.0.1 software versions that impacts connectivity of the following AP platforms with AirWave, when using certificate-based authentication: all AP-3XX, and AP-5XX, AP-203H, AP-203R, AP-203RP, and IAP-207. This issue is fixed in Instant 8.6.0.2.

Locally managed IAPs

- For IAPs managed using management options that are built into the AP, the impact is limited. The IAPs will continue to serve clients, pass traffic, and be managed locally. However, connectivity to Activate will be lost. This will imply that IAPs will not be able to synchronize on

any new provisioning rules in Activate and will not be able to get new image information automatically from Activate for upgrade, using local WebUI.

Additional Use Cases

- There is no impact of this issue in controller-based AP (CAP) deployments. APs terminating on Aruba controllers are defined as CAPs and run ArubaOS software. This defect applies only to Instant software (Instant OS) and does not impact ArubaOS.

- The current (Instant OS 8.5.0.3) and previous (Instant OS 6.5.4.3) manufacturing images used by the factory to build new APs have this bug. New deployment of APs in factory default state would potentially exhibit this issue. However, check the fourth bullet in Customer Deployments Not Affected section (above) to understand how Activate will be able to force an upgrade of APs in factory default state to a software image with the fix, so the deployment can proceed without any problem.

- The factory is in the process of updating the AP manufacturing image to a version with the fix.

- Customers with Instant deployments (without an official software image) running an existing c-build will be impacted.

ARUBA TECHNICAL ASSISTANCE CENTER

Should you require any assistance or clarification regarding this advisory, you can open a support case through the Aruba Support Portal at https://asp.arubanetworks.com. To call, please use the numbers found @ https://www.arubanetworks.com/support-services/contact-support/

This Support Advisory will be posted on the Aruba Support Site under the Announcements section and may be revised as applicable. Ensure that you check again for further updates.

Aruba is committed to communicating code revision, feature, and function recommendations to ensure optimal network operation and high customer satisfaction. The Aruba Global Support team can facilitate further product related discussions with the Product Management team for customers who desire to do so.

Thank you,

Aruba Global Support Services
