各位尊敬的客户以及合作伙伴：

Aruba 今天官方正式发布了有关 Aruba Instant AP 证书到期问题的技术支持建议。本技术支持建议发布在 Aruba support 网站上的公告栏目下，并且还将在今晚通过电子邮件发送给所有客户和合作伙伴。

请您仔细阅读本文中的内容，如果您部署的 IAP 网络属于受影响的部署方案之一，请在 2020 年 2 月 7 日之前将您的 IAP 升级到已修复该问题的新 IAP 软件版本。

请注意：如果您部署的 IAP 网络中运行的是 Instant OS C-Build 软件版本，建议您将 IAP 升级到推荐的主线版本之一。否则，请与 Aruba 技术团队联系，提供有关客户部署的详细信息。

请详细阅读本文的相关内容，如果您有任何疑问，请告知我们。

Aruba Support Advisory ARUBA-SA-20191219-PLVL08

Aruba Instant Certificate Expiry Issue

Aruba Instant AP 证书到期问题

概述

有一个软件 bug 可能会影响到 Aruba IAP 访问 Aruba Central，Activate 和 AirWave 服务。此软件 bug 与 IAP 软件版本中的 Trust Anchor（TA）文件中的 SSL 证书相关，如果没有采用有效修复措施，在 2020 年 2 月 7 日之后，可能会导致 IAP 与管理平台的连接断开。这不是安全漏洞，但是该软件缺陷可能会导致 AP 失去与管理平台的连接。

问题说明

该问题的起因是 IAP 中的 TA 证书包中的一个 Verisign 证书将于 2020 年 2 月 7 日到期。尽管 IAP 的软件版本中包含此证书的更新版本，但如果遇到单个已过期的证书，SSL 库中的一个软件缺陷将忽略所有有效证书。现有的 IAP 部署将因为此缺陷无法建立与 Central，Activate 和 AirWave 的 SSL 连接。

请注意：IAP 在没有这些管理服务的情况下仍能正常运行，即该问题并不会影响实际的网络业务，即 IAP 在 2020 年 2 月 7 日之后仍能保持功能正常并转发流量。此外，现有的 Central 和 AirWave 会话将在 2020 年 2 月 7 日之后保持活动状态。但如果 AP 和管理平台的连接发生断开或重置了任何的 Central 或 AirWave 服务，IAP 和管理平台之间的连接将不会保持活动状态，并且 IAP 将恢复为本地管理模式。要重新连接到管理服务平台，需要对每个 IAP 集群和每个 standalone 模式的 IAP 进行手动升级，以加载补丁程序，以重新建立与 Central，Activate 或 Airwave 的连接。由于上述问题，我们强烈建议所有受影响的客户在 2020 年 2 月 7 日之前升级到具有此修复程序的软件版本。

受此影响的产品

所有需要连接到 Central，Activate 和 Airwave 的 IAP 都有可能受到影响

受影响的软件版本 (目前仍在技术支持范围内的版本)	受影响的 IAP 硬件平台
Instant 8.6.0.0 之前的所有版本(8.5.x.x, 8.4.x.x, 8.3.x.x, 6.5.x.x, 6.4.x.x-4.2.x.x)	所有 IAP 平台(IAP-1XX, 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

不受影响的产品

Software Version	IAP Platforms
所有运行在 Instant 8.6.0.0 的 AP	All AP-3XX, and AP-5XX, AP203H/203R/203RP, and IAP-207
控制器架构下的 CAP 以及 RAP	

受影响的客户部署架构

使用受影响的 Instant AP 以及受影响的 IAP 软件版本进行的网络部署，连接到以下任意一项管理平台：

- Aruba Central
- Aruba Activate
- 具有基于证书的身份验证的 Airwave。据统计，实际部署的 IAP 中只有不到 10%使用此选项。

对使用不同管理平台对客户部署实际影响的详细信息，请参阅本文后续标题为“由于此缺陷导致的对客户影响的详细细节”的部分。
注意：满足上述任一条件的 C-build IAP 部署也会受到影响。

不会受影响的客户部署

此问题不会影响以下采用 Instant AP 的部署方案。

- 使用基于 PSK 的设备身份验证进行 Airwave 管理的部署
- 不使用 Central，Airwave 或 Activate，而是在本地管理的 Instant AP
- AP 处于默认出厂设置，未经过任何配置的 Instant AP
    - 如果未经配置的，处于出厂默认状态的 AP 部署在提供 Internet 连接的场景，可以使 AP 能访问到‘Activate’服务的环境中，则 Activate 将能够对该设备进行强制升级，升级到可以修复该问题的一个软件版本。然后升级后的 AP 将重新联网，与 Activate 设置安全连接，然后继续进行下一步，包括成功重定向到 Aruba Central 或 AirWave。
    - 如果处于出厂默认设置的 AP 部署在无法连接 Internet 的环境中，则 AP 不能访问 Activate 服务，那么将无法自动执行 AP 升级。在这种情况下，客户必须手动将 AP 升级到具有此修复程序的软件版本。
- 基于控制器的 AP 部署

- 如果在新的基于控制器的部署中 AP 可以使用 Internet 连接，则 AP 仍会与 activate 建议连接，然后 activate 将强制将 AP 升级到具有此修复程序的软件版本。升级后，AP 将连接到控制器。
- 如果 Internet 连接不可用，则 AP 将仍然能够连接到控制器。

不采取修复措施会造成的影响

如果受到影响的客户在 2020 年 2 月 7 日仍然没有升级：

- IAP 将继续为客户端提供连接以及转发流量，不会影响用户的实际上网业务。
- IAP 与 Central 以及 Airwave 的现有连接将继续保持不变，直到 2020 年 2 月 7 日之后。但是，如果由于互联网连接中断，Airwave 重启或 Central 的重置而重新设置了该连接，受影响的 IAP 将无法重新建立与管理平台的新 SSL 连接。此问题仅影响 IAP 与管理平台之间的连接。

解决方案

此证书过期的 bug 已经在以下的软件版本得到修复：

Instant Patch	Release Date
6.4.4.8-4.2.4.16	20-Dec-2019
6.5.4.15	20-Dec-2019
8.3.0.11	20-Dec-2019
8.4.0.6	16-Dec-2019 (Posted)
8.5.0.5	09-Dec-2019 (Posted)
8.6.0.1	20-Dec-2019

升级到以上目标版本可以修复此问题

请注意以下事项：

- Instant OS 6.5.x.x-4.3.x.x 和 6.5.3.x 的 release 版本已停止支持。建议运行这两种软件版本之一的客户升级到 Instant OS 6.5.4.15。
- Instant OS 6.4.4.8-4.2.xx 是 RAP-3，RAP-108，RAP-109，IAP-103，IAP-104，IAP-105，IAP-134，IAP135 和 IAP- 175 的最后一个支持版本。建议使用这些 AP 平台的客户升级到 Instant OS 6.4.4.8-4.2.4.16。
- Instant OS 6.5.4.x 是 IAP-204，IAP-205，IAP-205H，IAP-114 和 IAP-115 的最后支持版本。建议使用这些 AP 平台的客户升级到 Instant OS 6.5.4.15。
- Instant 8.6.x.x 是 RAP-155，IAP-214，IAP-215，IAP-224，IAP-225，IAP-228，IAP-274，IAP-275，IAP-277 的最后支持版本。因此，建议使用这些 AP 平台的客户升级到 Instant 8.6.0.1。
- 运行 c-build 的客户需要升级到具有错误修复的软件补丁之一（如适用）。您可以与 Aruba 技术团队或 Aruba 全球支持联系。
- 对于部署了 FIPS 版本的 IAP 的客户，将提供带有此修复程序的新 FIPS 版本的软件。

Aruba Central 管理下的 IAP 集群软件升级测试

- 在 Aruba 的测试中，由 Central 通过 1Mbps（最坏的情况）互联网链路管理的 128 个 IAP 的集群的软件版本升级，用不到 15 分钟的时间即可升级所有 IAP。
- 升级前检查和升级后验证需要 15 分钟，因此平均应该在 30 分钟内完成 128 个 IAP 集群升级。

由于此缺陷导致的对客户影响的详细细节

如果 IAP 的软件版本未在 2020 年 2 月 7 日之前升级到推荐版本，则下面列出的是将受此问题影响的管理服务选项。

Activate 连接

- 所有具有 Internet 连接的 IAP 都会连接到“Activate”以获取零接触配置（ZTP）规则。此外，IAP 会定期与 Activate 进行连接，以同步配置规则和可用的软件版本。如果不运行推荐的软件版本之一，IAP 将失去与 Activate 的连接，继续为客户端提供服务，并维持集群内的用户业务流量。在将 IAP 集群升级到具有此修复程序的软件版本之前，将无法使用“activate”的定期同步。

Central 管理下的 IAPs

- 对于由 Central 管理的 IAP，重置连接后 AP 将失去与 Central 的连接。但 AP 将继续为客户端提供接入服务，用户的实际上网业务并没有任何影响。但是，IAP 到 Central 将不可访问，并且将退回到 IAP 本地管理。要恢复与 Central 的连接，需要将 IAP 集群手动升级到带有此修复程序的软件版本。
- 由于多种原因，包括 Internet 连接问题、IAP 的重新启动以及 Central 升级，都可能会重置 IAP 与 Central 之间的现有连接。
- 如果由于任何原因重置了 Central 连接，则 Central 将无法访问 IAP。这将影响所有未在 2020 年 2 月 7 日之前将受影响的 IAP 升级到具有此修复程序的软件版本的 Central 客户。

Airwave 管理下的 IAPs

- 根据所选的身份验证方法（基于证书或基于 PSK）重置现有连接后，将对 Airwave 托管的 IAP 部署产生影响。
- 对于在 Airwave 和 IAP 之间使用基于证书的身份验证选项的客户，当重置现有连接时，将失去与 Airwave 的连接。
- 对于在 Airwave 和 IAP 之间使用基于 PSK 的身份验证选项的客户，没有影响。
- 由于多种原因，IAP 和 Airwave 之间的现有连接可能会重置，包括 IAP 和 Airwave 之间的 LAN 或 WAN 连接问题，IAP 的重新启动，Airwave 的重新启动以及 Airwave 软件的升级。

本地管理模式下的 IAPs

对于使用本地管理模式的 IAP，其影响是有限的。 IAP 将继续为客户提供服务，转发流量并在本地进行管理。但是，到‘Aruba Activate’的连接将丢失。这意味着 IAP 将无法在 Activate 中的任何新配置规则上进行同步，也将无法使用本地 WebUI 中自动获取新的映像信息进行升级。

补充说明

- 在基于控制器的 AP（CAP）部署中，此问题没有影响。此缺陷仅适用于 Instant 软件（Instant OS），不会影响 ArubaOS。
- Aruba 当前的 IAP 出厂版本 Instant OS 8.5.0.3，以及以前的出厂版本 Instant OS 6.5.4.3 均存在此问题。出厂默认状态下新部署的 AP 可能会出现此问题。但是请查看“不受影响的客户部署”部分中的第三大项，以了解“Activate”如何将处于出厂默认状态的 AP 强制升级到具有修复程序的软件映像，因此部署可以顺利进行。
- Aruba 工厂已经在将 AP 出厂时的软件镜像更新为带有修复程序的版本。
- 运行现有 c-build 版本的 Instant（无官方软件映像）客户将受到影响。