# Sécurité : Aruba Networks panse ses plaies

Aruba Networks a alerté que plusieurs de ses logiciels sont affectés de quelques 26 vulnérabilités au total. Lesquelles peuvent permettre de l'exécution de code à distance, de la fuite d'information, et éclairent l'absence de sécurité dans les mécanismes de mise à jour et le stockage d'identifiants et clés privées de chiffrement. L'ensemble de ces failles sont référencées CVE-2016-2031 et CVE-2016-2032.

Sont affectés ArubaOS, AirWave Management Platform (AMP) et Aruba Instant (IAP). L'origine des failles de sécurité se trouve principalement dans le système de gestion et de contrôle du protocole propriétaire PAPI commun aux trois logiciels. *« Le protocole PAPI contient un certain nombre de défauts non résolus, dont : les messages 'hachés' MD5 ne sont pas correctement validées lors de la réception, le chiffrement du protocole PAPI est faible; tous les périphériques Aruba utilisent une clé statique commune pour la validation du message »*, précise le fournisseur de solutions de communications sans fil dans une de ses alertes.

## Failles découvertes par Google

Auba reconnait avoir publié ses notifications sous la pression de Google. *« Le contenu de cet avis est soumis à une divulgation publique imminente par l'équipe de sécurité de Google dans un délai de divulgation de 90 jours*, avance le fournisseur dans son alerte consacrée à Aruba Instant. *Par conséquent, les clients sont invités à traiter de toute urgence cet avis. »* L'entreprise craint que la divulgation des détails des vulnérabilités attire désormais l'attention de la communauté des attaquants. Mais n'en remercie pas moins le chercheur Sven Blumenstein de la Google Security Team pour ses trouvailles.

Pour la filiale de HPE depuis mars 2015, certaines des vulnérabilités ne peuvent pas être corrigées immédiatement. Elles le seront dans le courant du troisième trimestre à travers le changement de PAPI afin d'opérer les communications avec un canal sécurisé tel que IPsec ou DTLS. En attendant, Aruba invite ses clients à installer les versions IAP 4.1.3.0 ou 4.2.3.1 qui corrige certaines des brèches évoquées (mais pas toutes). Ou encore de se reporter à la documentation « Control Plane Security Best Practices » pour protéger au mieux leurs infrastructures. *« Selon la configuration du réseau et la tolérance au risque, aucune action n'est peut-être nécessaire »*, estime Aruba.

---

**Lire également**
Les ransomwares tirent et réclament à tout va
Attaques DDoS : bluffer suffit pour bien gagner
Robinson Delaugerre, Verizon : « Les menaces n'ont pas fondamentalement changé »