
# BULLETIN DE VEILLE N°10

ANPT-2025-BV-10

**"The human factor is the weakest link in cybersecurity.."**
**— Bruce Schneier**

Octobre 2025

# Alertes de sécurité

## Vmware

### Plusieurs vulnérabilités dans VMware Aria Operations et VMware Tools pourraient permettre une élévation des privilèges

**30 Octobre 2025**

Plusieurs vulnérabilités ont été identifiées dans VMware Aria Operations et VMware Tools, la plus grave permettant une élévation de privilèges jusqu'au niveau root. L'instance Aria Operations, plateforme de gestion multi-cloud (public, privé, hybride) pour l'infrastructure et les applications, est impactée. Le scénario d'attaque principal (CVE-2025-41244) permet à un utilisateur malveillant local, non-administrateur, disposant d'un accès à une machine virtuelle où VMware Tools est installé et géré par Aria Operations avec le pack SDMP activé, d'augmenter ses privilèges pour devenir root sur cette VM. L'exploitation réussie permettrait à l'attaquant d'installer des programmes, de consulter, modifier ou supprimer des données, ou encore de créer de nouveaux comptes avec droits complets sur le système.

D'autres vulnérabilités accompagnent cette faille : CVE-2025-41245 permet à un acteur local non-administrateur dans Aria Operations de divulguer les identifiants d'autres utilisateurs, tandis que CVE-2025-41246 permet à un acteur non-administrateur sur une VM invitée, déjà authentifié via vCenter ou ESX, d'accéder à d'autres machines virtuelles invitées, sous réserve de connaître certains identifiants. Ces vulnérabilités cumulées élargissent la surface d'attaque dans les environnements virtualisés. Le risque est classé comme élevé pour les grandes et moyennes structures (gouvernement ou entreprises) et moyen pour les plus petites.

Pour atténuer ces risques, CIS recommande : appliquer immédiatement les correctifs fournis par Broadcom Inc./VMware (versions fixées : Aria Operations 8.18.5, Cloud Foundation Operations 9.0.1.0, VMware Tools 12.5.4 ou 13.0.5 selon les plateformes) ; mettre en œuvre un processus de gestion des vulnérabilités robuste et documenté, avec scans réguliers, mises à jour fréquentes et réseau segmenté ; adopter le principe du moindre privilège, gérer les comptes par défaut et passer en revue les comptes de service. Il n'existe pour l'instant aucun contournement (workaround) fiable pour ces vulnérabilités, ce qui rend la mise à jour absolument prioritaire

***Source :*** ***https://bit.ly/49dwaia***

## Apple

### Google Project d'Apple « Zero Exposes ASLR Bypass » révèle une vulnérabilité dans le cadre de sérialisation d'Apple

**2 octobre 2025**

Les chercheurs de Google Project Zero ont révélé une nouvelle méthode permettant de contourner la protection ASLR (Address Space Layout Randomization), essentielle à la sécurité mémoire des systèmes modernes. Cette attaque combine des fuites micro-architecturales, des mesures de latence et des observations comportementales pour déduire les adresses mémoire sans provoquer de crashs visibles. En réduisant fortement l'entropie d'ASLR, elle permet à un attaquant de localiser des zones critiques et exécuter du code arbitraire avec une grande fiabilité. Les tests effectués sur plusieurs plateformes ont prouvé que même les systèmes considérés comme sécurisés restaient vulnérables face à cette approche multi-étape.

Selon Project Zero, les contre-mesures classiques comme DEP ou CFI ne suffisent pas à stopper cette attaque, car elle exploite des failles intrinsèques au matériel et au cache processeur. Les chercheurs recommandent d'augmenter l'entropie d'ASLR, de renforcer l'isolation mémoire et d'activer les protections avancées du compilateur. Dans les environnements sensibles, ils conseillent aussi de segmenter les charges critiques, de surveiller les comportements mémoire inhabituels et d'appliquer les mises à jour microcode disponibles. Cette découverte illustre la fragilité des protections existantes et la nécessité d'une défense en profondeur contre les attaques exploitant les mécanismes internes du processeur.

***Source :*** ***https://bit.ly/49dwaia***

# Actualité

### Le piratage du fournisseur américain de services de surveillance RemoteCOM expose des données judiciaires

Un piratage majeur a frappé RemoteCOM, une société américaine spécialisée dans les technologies de surveillance judiciaire, exposant des milliers de données sensibles. L'incident a révélé plus de 14 000 dossiers personnels de personnes sous surveillance ainsi que près de 7 000 enregistrements liés à des membres des forces de l'ordre. Les données compromises comprenaient des noms, adresses, numéros de téléphone, adresses e-mail, identifiants, adresses IP et plus de 380 000 alertes d'activité issues du logiciel de surveillance SCOUT. Ce programme, utilisé pour suivre les individus placés sous contrôle, fonctionne comme un véritable outil d'espionnage numérique, capable d'enregistrer les frappes clavier, de suivre la localisation et de capturer des images d'écran.

Le pirate, utilisant le pseudonyme "wikkid", a affirmé que l'attaque avait été « facile », suggérant un manque de mesures de sécurité fondamentales chez RemoteCOM. Les fichiers divulgués, nommés "Clients" et "Officers", contenaient non seulement des informations personnelles, mais aussi des notes internes, des rapports d'activité et des données techniques sur les dispositifs de suivi. Certaines preuves indiquent que des téléphones appartenant à des proches d'agents de l'État ont été surveillés, révélant des erreurs graves et soulevant des questions éthiques sur les pratiques de surveillance électronique. L'attaque démontre combien la centralisation de telles données dans des systèmes mal protégés peut devenir une menace pour la vie privée et la sécurité nationale.

Les conséquences de cette fuite sont préoccupantes : risque d'usurpation d'identité, de chantage, et de ciblage de fonctionnaires. Les données des agents exposés pourraient être exploitées à des fins de harcèlement ou d'attaques ciblées. RemoteCOM affirme avoir ouvert une enquête interne et travaille avec des experts pour déterminer la cause de la compromission. Les spécialistes en cybersécurité recommandent une révocation immédiate des identifiants compromis, un chiffrement renforcé des bases de données, et une notification rapide des personnes concernées. Cet incident rappelle la nécessité de soumettre les entreprises privées de surveillance à des normes de sécurité strictes, afin d'éviter que de telles brèches n'exposent à nouveau des informations aussi sensibles.

***Source :*** https://bit.ly/4axx6iA

### L'opérateur du réseau électrique suédois confirme la violation de données revendiquée par un groupe de ransomware

Un incident de cybersécurité a touché Svenska kraftnät, l'opérateur national suédois du réseau de transport d'électricité, qui a confirmé une atteinte à un système externe de transfert de fichiers sans impact sur l'alimentation électrique nationale. La faille a été découverte samedi et a immédiatement déclenché une enquête interne tandis que l'agence notifiait les autorités compétentes pour coordination et poursuite des investigations. L'opérateur indique qu'il n'y a, à ce stade, aucune indication que les systèmes critiques de l'infrastructure électrique aient été affectés, mais l'évaluation complète du périmètre des données exposées est toujours en cours.

Un groupe se présentant comme le ransomware Everest a revendiqué la compromission sur son site de fuite, affirmant l'exfiltration d'environ 280 Go de données internes et menaçant de publication si ses exigences n'étaient pas respectées.

Les fichiers volés proviendraient d'un stockage lié à un outil de transfert externe — un vecteur fréquemment ciblé car souvent moins surveillé et isolé.

Svenska kraftnät a précisé que l'attaque avait compromis un système externe isolé plutôt que la plateforme opérationnelle centrale du réseau. L'organisation a isolé la ressource affectée, lancé des audits forensiques et coopère avec la police et les autorités nationales de cybersécurité pour déterminer l'origine et l'ampleur de la fuite.

Les communications publiques restent prudentes : l'opérateur retient des détails afin de ne pas entraver l'enquête en cours ni fournir d'indications aux attaquants.

Même si les opérations de transport d'électricité ne semblent pas touchées, l'exfiltration de centaines de gigaoctets peut contenir des informations sensibles : contrats, plans, accès d'administration, journaux d'audit ou données de maintenance. La divulgation publique de ces éléments exposerait l'opérateur et ses partenaires à des risques accrus d'ingénierie sociale, d'extorsion, et de campagnes ciblées contre des infrastructures ou des personnels. Les recommandations immédiates sont classiques mais impératives : inventorier et protéger les systèmes externes de transfert, révoquer et faire tourner les identifiants compromis, chiffrer les sauvegardes, et mener des contrôles d'accès renforcés.

À moyen terme, il faut segmenter strictement les environnements d'échange de fichiers, appliquer le principe du moindre privilège et renforcer la surveillance détective autour des flux sortants et des connexions tierces.

***Source : https://bit.ly/4arUdea***

# Bon à savoir

### La protection des données personnelles dans l'entreprise

Dans le monde professionnel actuel, la protection des données personnelles est la responsabilité de tous, pas seulement du service informatique. Chaque employé manipule des informations sensibles, qu'il s'agisse de dossiers clients, de données financières ou de coordonnées internes. Une simple erreur, comme envoyer un courriel à la mauvaise personne ou laisser un

fichier ouvert à l'écran, peut avoir de graves conséquences. Les données personnelles comprennent tout ce qui permet d'identifier une personne : nom, adresse, numéro de téléphone ou pièce d'identité. Traitez ces informations avec le même soin que vous souhaitez pour vos propres données. Pensez à verrouiller votre ordinateur lorsque vous quittez votre poste et évitez de discuter d'informations confidentielles dans des lieux publics ou sur des canaux non sécurisés.

Lorsque vous traitez des données, suivez toujours les politiques de sécurité de votre entreprise et utilisez uniquement les outils autorisés pour stocker ou partager des fichiers. Ne sauvegardez jamais d'informations confidentielles sur des appareils personnels, des clés USB ou des services cloud non approuvés. Vérifiez que l'accès aux documents sensibles est limité aux personnes qui en ont réellement besoin. Avant d'envoyer une pièce jointe, assurez-vous que le destinataire est correct et que le partage est nécessaire. Évitez également d'imprimer des documents contenant des informations personnelles, sauf en cas d'obligation, et détruisez-les correctement après usage à l'aide de bacs de destruction sécurisée. Rappelez-vous : la commodité ne doit jamais passer avant la sécurité.

Enfin, restez vigilant face aux emails de phishing ou aux demandes de données inhabituelles. Les cybercriminels se font souvent passer pour des responsables, des collègues ou des prestataires afin d'obtenir des informations sensibles. Si un message semble suspect ou trop urgent, vérifiez toujours sa légitimité par un autre moyen avant de répondre. Signalez immédiatement toute fuite ou tentative d'accès non autorisé à votre service informatique ou à la direction. Protéger les données personnelles ne consiste pas seulement à suivre des règles, mais aussi à préserver la confiance de vos collègues, clients et partenaires. En restant attentif, responsable et prudent, vous contribuez directement à la sécurité numérique et à la réputation de votre entreprise.

# Evènements

## Evènement à venir

**International Conference on Machine Learning and Cybernetics (ICMLC)**

18 November 2025 | Setif, Algeria

https://www.sans.org/

L'International Conference on Machine Learning and Cybernetics (ICMLC) se tiendra le 18 novembre 2025 à Sétif, Algérie.

Cet événement réunira chercheurs, ingénieurs et universitaires autour des innovations en intelligence artificielle et cybernétique.

La conférence vise à promouvoir les échanges sur les applications réelles du machine learning.

Elle servira aussi de plateforme pour présenter des projets de recherche et des publications récentes.

Les participants pourront établir de nouvelles collaborations scientifiques.

L'ICMLC 2025 contribuera à renforcer la recherche en IA en Algérie et à l'international.