Synthèse de veille réglementaire

Export généré le 06/11/2026 à 03:37 · 6 texte(s) · Les filtres actifs de la page sont conservés.

Textes	6	Action requise	0	À analyser	2	Information	4

Information 29/10/2026 · Vigilance cyber · Cybersécurité des systèmes de sûreté

Bulletin d'actualité du CERT-FR

Résumé

? Ciblage de téléphones Apple ? Nouvelle campagne de notification le 29 octobre 2026 Bulletin d'actualité du CERT-FR Objet : Bulletin d'actualité CERTFR-2026-ACT-046 Imprimer Gestion du document Référence CERTFR-2026-ACT-046 Titre Bulletin d'actualité CERTFR-2026-ACT-046 Date de la première version02 novembre 2026 Date de la dernière version02 novembre 2026 Source(s) Une gestion de version détaillée se trouve à la fin de ce document. Ce bulletin d'actualité du CERT-FR revient sur les vulnérabilités significatives de la semaine passée pour souligner leurs criticités. Il ne remplace pas l'analyse de l'ensemble des avis et alertes publiés par le CERT-FR dans le cadre d'une analyse de risques pour prioriser l'application des correctifs. Toutes les vulnérabilités évoquées dans les avis du CERT-FR doivent être prises en compte et faire l'objet d'un plan d'action lorsqu'elles génèrent des r

Impact pour l’exploitant
Vigilance cyber susceptible d'affecter un équipement ou logiciel utilisé pour la sûreté physique, la vidéoprotection, le contrôle d'accès ou les systèmes techniques d'un site.

Actions recommandées

- Identifier si le produit concerné est présent dans le parc
- Vérifier les versions installées et les correctifs éditeur
- Évaluer l'exposition réseau et les accès d'administration
- Planifier la correction sans dégrader la continuité de la sûreté

Entrée en vigueur : Non précisée

Ouvrir la source officielle

Information 29/10/2026 · Vigilance cyber · Cybersécurité des systèmes de sûreté

Bulletin d'actualité du CERT-FR

Résumé

? Ciblage de téléphones Apple ? Nouvelle campagne de notification le 29 octobre 2026 Bulletin d'actualité du CERT-FR Objet : Bulletin d'actualité CERTFR-2026-ACT-036 Imprimer Gestion du document Référence CERTFR-2026-ACT-036 Titre Bulletin d'actualité CERTFR-2026-ACT-036 Date de la première version24 août 2026 Date de la dernière version24 août 2026 Source(s) Une gestion de version détaillée se trouve à la fin de ce document. Ce bulletin d'actualité du CERT-FR revient sur les vulnérabilités significatives de la semaine passée pour souligner leurs criticités. Il ne remplace pas l'analyse de l'ensemble des avis et alertes publiés par le CERT-FR dans le cadre d'une analyse de risques pour prioriser l'application des correctifs. Toutes les vulnérabilités évoquées dans les avis du CERT-FR doivent être prises en compte et faire l'objet d'un plan d'action lorsqu'elles génèrent des risques s

Impact pour l’exploitant
Vigilance cyber susceptible d'affecter un équipement ou logiciel utilisé pour la sûreté physique, la vidéoprotection, le contrôle d'accès ou les systèmes techniques d'un site.

Actions recommandées

- Identifier si le produit concerné est présent dans le parc
- Vérifier les versions installées et les correctifs éditeur
- Évaluer l'exposition réseau et les accès d'administration
- Planifier la correction sans dégrader la continuité de la sûreté

Entrée en vigueur : Non précisée

Ouvrir la source officielle

À analyser 28/10/2026 · Vigilance cyber · Cybersécurité des systèmes de sûreté

Avis du CERT-FR

Résumé

Violations de données applicatives – Le CERT-FR partage son expérience CERTFR-2026-CTI-008 Avis du CERT-FR Json Objet : Vulnérabilité dans Axis Camera Station Pro Gestion du document Référence CERTFR-2026-AVI-1408 Titre Vulnérabilité dans Axis Camera Station Pro Date de la première version28 octobre 2026 Date de la dernière version28 octobre 2026 Source(s) Bulletin de sécurité Axis cve-2026-63286pdf-en-US-560650 du 28 octobre 2026 Une gestion de version détaillée se trouve à la fin de ce document. Risque Atteinte à la confidentialité des données Systèmes affectés Camera Station Pro versions antérieures à 6.20 Résumé Une vulnérabilité a été découverte dans Axis Camera Station Pro. Elle permet à un attaquant de provoquer une atteinte à la confidentialité des données. Solutions Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation). Docum

Impact pour l’exploitant
Vigilance cyber susceptible d'affecter un équipement ou logiciel utilisé pour la sûreté physique, la vidéoprotection, le contrôle d'accès ou les systèmes techniques d'un site.

Actions recommandées

- Identifier si le produit concerné est présent dans le parc
- Vérifier les versions installées et les correctifs éditeur
- Évaluer l'exposition réseau et les accès d'administration
- Planifier la correction sans dégrader la continuité de la sûreté

Entrée en vigueur : Non précisée

Ouvrir la source officielle

À analyser 08/09/2026 · Vigilance cyber · Cybersécurité des systèmes de sûreté

Objet: Multiples vulnérabilités dans les produits SAP

Résumé

Premier Ministre S.G.D.S.N Agence nationalede la sécurité dessystèmes d'information Paris, le 08 septembre 2026 N° CERTFR-2026-AVI-1134 Affaire suivie par: CERT-FR Avis du CERT-FR Objet: Multiples vulnérabilités dans les produits SAP Gestion du document Référence CERTFR-2026-AVI-1134 Titre Multiples vulnérabilités dans les produits SAP Date de la première version08 septembre 2026 Date de la dernière version08 septembre 2026 Source(s) Bulletin de sécurité SAP september-2026 du 08 septembre 2026 Une gestion de version détaillée se trouve à la fin de ce document. Risques Atteinte à la confidentialité des données Contournement de la politique de sécurité Déni de service à distance Exécution de code arbitraire à distance Falsification de requêtes côté serveur (SSRF) Injection de requêtes illégitimes par rebond (CSRF) Injection SQL (SQLi) Non spécifié par l'éditeur Élévation de privilèges Syst

Impact pour l’exploitant
Vigilance cyber susceptible d'affecter un équipement ou logiciel utilisé pour la sûreté physique, la vidéoprotection, le contrôle d'accès ou les systèmes techniques d'un site.

Actions recommandées

- Identifier si le produit concerné est présent dans le parc
- Vérifier les versions installées et les correctifs éditeur
- Évaluer l'exposition réseau et les accès d'administration
- Planifier la correction sans dégrader la continuité de la sûreté

Entrée en vigueur : Non précisée

Ouvrir la source officielle

Information 24/08/2026 · Vigilance cyber · Cybersécurité des systèmes de sûreté

Objet: Bulletin d'actualité CERTFR-2026-ACT-036

Résumé

Premier Ministre S.G.D.S.N Agence nationalede la sécurité dessystèmes d'information Paris, le 24 août 2026 N° CERTFR-2026-ACT-036 Affaire suivie par: CERT-FR Bulletin d'actualité du CERT-FR Objet: Bulletin d'actualité CERTFR-2026-ACT-036 Gestion du document Référence CERTFR-2026-ACT-036 Titre Bulletin d'actualité CERTFR-2026-ACT-036 Date de la première version24 août 2026 Date de la dernière version24 août 2026 Source(s) Une gestion de version détaillée se trouve à la fin de ce document. Ce bulletin d'actualité du CERT-FR revient sur les vulnérabilités significatives de la semaine passée pour souligner leurs criticités. Il ne remplace pas l'analyse de l'ensemble des avis et alertes publiés par le CERT-FR dans le cadre d'une analyse de risques pour prioriser l'application des correctifs. Toutes les vulnérabilités évoquées dans les avis du CERT-FR doivent être prises en compte et faire l'o

Impact pour l’exploitant

Vigilance cyber susceptible d'affecter un équipement ou logiciel utilisé pour la sûreté physique, la vidéoprotection, le contrôle d'accès ou les systèmes techniques d'un site.

Actions recommandées

- Identifier si le produit concerné est présent dans le parc
- Vérifier les versions installées et les correctifs éditeur
- Évaluer l'exposition réseau et les accès d'administration
- Planifier la correction sans dégrader la continuité de la sûreté

Entrée en vigueur : Non précisée

Ouvrir la source officielle

Information 29/06/2026 · Vigilance cyber · Cybersécurité des systèmes de sûreté

Objet: Bulletin d'actualité CERTFR-2026-ACT-028

Résumé

Premier Ministre S.G.D.S.N Agence nationalede la sécurité dessystèmes d'information Paris, le 29 juin 2026 N° CERTFR-2026-ACT-028 Affaire suivie par: CERT-FR Bulletin d'actualité du CERT-FR Objet: Bulletin d'actualité CERTFR-2026-ACT-028 Gestion du document Référence CERTFR-2026-ACT-028 Titre Bulletin d'actualité CERTFR-2026-ACT-028 Date de la première version29 juin 2026 Date de la dernière version29 juin 2026 Source(s) Une gestion de version détaillée se trouve à la fin de ce document. Ce bulletin d'actualité du CERT-FR revient sur les vulnérabilités significatives de la semaine passée pour souligner leurs criticités. Il ne remplace pas l'analyse de l'ensemble des avis et alertes publiés par le CERT-FR dans le cadre d'une analyse de risques pour prioriser l'application des correctifs. Toutes les vulnérabilités évoquées dans les avis du CERT-FR doivent être prises en compte et faire l'o

Impact pour l’exploitant

Vigilance cyber susceptible d'affecter un équipement ou logiciel utilisé pour la sûreté physique, la vidéoprotection, le contrôle d'accès ou les systèmes techniques d'un site.

Actions recommandées

- Identifier si le produit concerné est présent dans le parc
- Vérifier les versions installées et les correctifs éditeur
- Évaluer l'exposition réseau et les accès d'administration
- Planifier la correction sans dégrader la continuité de la sûreté

Entrée en vigueur : Non précisée

Ouvrir la source officielle