Cybersecurity Database

Rapport

ARTEX, l'outil d'attaque piloté par l'intelligence artificielle signalé par le FBI et le CERT-EU (2026)

ARTEX est né comme un outil open source de tests d'intrusion automatisés piloté par des modèles de langage, mais depuis août 2026 des groupes criminels et étatiques l'utilisent contre des organisations du monde entier. Le CERT-EU a donné l'alerte le 5 novembre et le FBI le 13 novembre ; le 19 novembre, la Commission européenne a confirmé une campagne cyber menée avec un outil d'IA, qui selon elle a conduit le 23 novembre au vol de données des utilisateurs d'EU Academy. Ce que l'on sait, quelles règles et normes comptent et que faire tout de suite.

Édition Données au 27 novembre 2026

Version toujours à jour https://www.cybersecuritydatabase.org/fr/reports/artex-ai-hacking-tool/

Licence CC BY 4.0 : libre réutilisation avec mention de la source

À qui il s'adresse: Pour les journalistes et pour ceux qui travaillent dans les secteurs touchés : les faits confirmés par les sources officielles, les règles et normes associées et les mesures recommandées par les autorités.

> ARTEX est une plateforme de tests d'intrusion « autonome » : l'utilisateur décrit l'objectif avec des mots et une équipe d'agents fondés sur des modèles de langage mène seule la reconnaissance, l'exploitation des failles et l'exfiltration des données. Publiée sur GitHub en juillet 2026 pour des tests autorisés, elle est utilisée depuis août par des criminels et des groupes étatiques : selon le FBI, certaines intrusions sont passées du premier contact aux privilèges d'administrateur en moins de trois heures. Le dépôt a été retiré le 8 octobre, mais des copies, des variantes et une version commerciale circulent encore. Le CERT-EU le 5 novembre et le FBI le 13 novembre ont averti que sa diffusion accélère les attaques contre les systèmes exposés sur internet. Le 19 novembre, la Commission européenne a confirmé avoir subi, depuis octobre, une « campagne cyber générée par l'IA » ; le 23 novembre, elle a confirmé la fuite des noms et adresses e-mail des utilisateurs de la plateforme EU Academy. Le 24 novembre, la Suisse a aussi confirmé ses premières attaques réussies avec des agents d'IA contre des infrastructures critiques, et le 26 novembre le BSI allemand a averti que ces outils sont désormais mûrs pour un usage à grande échelle.

< 3 h
du premier contact aux privilèges d'administrateur, dans certaines intrusions (FBI)

1600+
consoles ARTEX exposées sur internet début novembre (FBI)

2250+
clients en aval visés dans l'attaque de la chaîne d'approvisionnement de ConnectWise (FBI)

Que faire tout de suite

Les recommandations du FBI et du CERT-EU pour réduire le risque d'une attaque menée avec ARTEX ou des outils semblables.

1. Inventorier tout ce qui est exposé sur internet, y compris les portails des partenaires et fournisseurs, les backends d'applications mobiles, les applications créées par chaque service et les anciens services, et éteindre ce qui ne sert pas.
2. Ne rendre les consoles d'administration du cloud et du réseau, les plateformes de sauvegarde et les autres services sensibles accessibles que depuis des réseaux de confiance ou des canaux dédiés, pas depuis internet.
3. Appliquer les correctifs d'urgence aux systèmes exposés et ne pas laisser en suspens les vulnérabilités jugées mineures : un outil automatique les enchaîne.
4. Utiliser l'authentification multifacteur et le moindre privilège pour les comptes et applications, et surveiller les nouveaux identifiants, les attributions de privilèges et les connexions depuis des réseaux inconnus.
5. Ne pas afficher de messages d'erreur détaillés aux utilisateurs non authentifiés, rechercher et remplacer les identifiants restés dans le code et les chaînes CI/CD, limiter le débit des API et des portails.

6. Conserver les journaux de connexion et d'audit, surveiller l'usage des outils d'IA sur son réseau et signaler un incident suspect impliquant ARTEX aux autorités (en Europe le CSIRT national, aux États-Unis l'IC3).

Chronologie

Date	Ce qui s'est passé	Sources
8 octobre 2026	Le développeur « Autumn-27 », qui avait publié ARTEX sur GitHub en juillet en le déclarant destiné aux seuls tests autorisés, rend le dépôt indisponible après des signalements d'usage par des attaquants. Selon le FBI, l'outil reste toutefois accessible via des forks, des copies archivées et une version commerciale, ARTEX PRO ; des attaques avec ARTEX sont observées depuis au moins août 2026.	[1]
5 novembre 2026	Le CERT-EU, service de cybersécurité des institutions de l'UE, publie l'analyse « Beware of ARTEX » : plusieurs acteurs malveillants dans le monde utilisent l'outil, et le CERT-EU a observé contre les institutions qu'il protège des activités semblables, pilotées par l'IA, très probablement menées avec ARTEX. La disponibilité publique de l'outil, avertit-il, en accélérera l'adoption.	[2]
13 novembre 2026	Le FBI diffuse l'alerte FLASH-20261113-001 sur ARTEX, avec les techniques observées, des indicateurs de compromission et des recommandations. Les secteurs touchés vont des services financiers à l'administration publique, de la défense aux semi-conducteurs, de l'énergie à la santé ; parmi les campagnes citées, une attaque contre des établissements financiers sud-coréens et la compromission de la chaîne d'approvisionnement de ConnectWise Cloud Backup. Le FBI demande de signaler à l'IC3 les incidents impliquant ARTEX.	[1]
19 novembre 2026	Au briefing de midi, le porte-parole de la Commission européenne confirme une « campagne cyber » contre la Commission, détectée le 22 octobre et confirmée le 26 octobre après les premières vérifications : par précaution, plusieurs applications ont été arrêtées et la plupart ont déjà été rétablies. Il s'agit d'une campagne « générée par l'IA », avec un outil d'IA accessible au public ; à ce stade, aucune preuve d'une violation des données de l'ensemble du personnel ni de demande de rançon connue. La Commission est en contact avec le CERT-EU et le Contrôleur européen de la protection des données et ne désigne pas de responsable.	[5]
23 novembre 2026	La Commission confirme que la campagne a aussi touché la plateforme EU Academy, qui propose des cours en ligne sur les politiques de l'UE à des utilisateurs externes : des données personnelles des utilisateurs, dont des noms et adresses e-mail, ont fuité. L'ampleur reste à établir ; l'accès public à la plateforme a été suspendu, les utilisateurs ont été prévenus par un message sur le site et le Contrôleur européen de la protection des données a été informé. Pas d'attribution tant que l'enquête n'est pas terminée.	[6]
24 novembre 2026	Le Centre national pour la cybersécurité suisse (NCSC/OFCS) confirme les premiers cas en Suisse d'attaques menées avec des agents d'IA (« Agentic Offensive Frameworks ») contre des entreprises et des exploitants d'infrastructures critiques d'au moins deux secteurs : dans tous les cas connus, les attaquants ont réussi à compromettre les systèmes. Selon le NCSC, les agents d'IA accessibles depuis internet, comme ARTEX ou CyberStrikeAI, ont presque doublé depuis octobre 2026 ; il recommande d'installer les mises à jour critiques des systèmes exposés sous 24 heures.	[3]

Date	Ce qui s'est passé	Sources
26 novembre 2026	L'Office fédéral allemand de la sécurité des technologies de l'information (BSI) avertit que les « Agentic Offensive Frameworks » comme ARTEX, CAIRN ou PentAGI sont passés de l'expérimentation à l'usage opérationnel et, sur la base de ses propres constats, confirme leur haut degré de maturité. Ils fonctionnent même avec des modèles librement disponibles et abaissent fortement les compétences nécessaires ; le BSI prévoit une forte hausse de la qualité et du nombre des attaques et estime que les infrastructures accessibles depuis internet seront compromises si les vulnérabilités ne sont pas corrigées. Il demande de supprimer les mots de passe faibles ou par défaut et les interfaces non protégées, d'avoir un plan d'urgence et de fermer sans attendre les voies d'attaque les plus simples.	[4]

Pays touchés et état des règles de l'UE

Pays	Cas signalés	SRI 2	CER
Union européenne	Le CERT-EU a observé contre les institutions, organes et agences de l'UE des activités pilotées par l'IA, très probablement menées avec ARTEX. La Commission européenne a confirmé une campagne « générée par l'IA », détectée le 22 octobre, avec un outil d'IA accessible au public, sans le nommer ; selon la presse, le CERT-EU y a reconnu ARTEX. Plusieurs applications internes ont été arrêtées par précaution (selon la presse, pendant plus de dix jours les systèmes de paie, de congés et de remboursements médicaux et les services de traduction : The Record, 19 novembre). Le 23 novembre, la Commission a confirmé le vol des noms et adresses e-mail des utilisateurs externes de la plateforme EU Academy, désormais fermée au public. [2] [5] [6] [7]	–	–
Corée du Sud	Selon le FBI, des attaques à but lucratif menées avec ARTEX contre des établissements financiers sud-coréens ont conduit à l'exfiltration des données personnelles d'environ 67 000 personnes. [1]	–	–
Suisse	Le NCSC suisse a reçu les premiers signalements d'attaques menées avec des agents d'IA contre des organisations et des exploitants d'infrastructures critiques d'au moins deux secteurs, toutes réussies ; il partage avec les exploitants d'infrastructures critiques les indicateurs techniques pour les détecter. [3]	–	–

Pays	Cas signalés	SRI 2	CER
Allemagne	Le BSI signale la multiplication des incidents où l'usage de ces outils est soupçonné, et en partie prouvé, et confirme sur la base de ses propres constats le haut degré de maturité des « Agentic Offensive Frameworks ». [4]	Transposée, en vigueur	Transposée, en vigueur

L'état de SRI 2 et de CER provient des pages de transposition du site et se met à jour avec les données.

Comment fonctionne ARTEX

Selon le FBI, ARTEX est une plateforme multi-agents écrite en Go qui traduit des objectifs décrits en langage naturel en commandes exécutées par des agents spécialisés, avec une intervention humaine minimale une fois l'objectif fixé. Elle ne contient pas de modèle propre : elle se connecte à des modèles de langage externes, commerciaux ou open source. Dans les instances contrôlées par les attaquants analysées par le FBI, les modèles d'origine chinoise dominent, choisis pour leur coût et leurs capacités et pour l'absence de garde-fous visibles lorsque la demande est présentée comme un test d'intrusion.

L'outil est particulièrement efficace sur les systèmes périphériques : portails des partenaires et fournisseurs, backends d'applications mobiles, applications pour les salariés, anciens services, intégrations avec des tiers. Parmi les techniques observées par le FBI figurent l'usage d'identifiants cloud exposés, des assertions SAML non signées, des failles XXE et SSRF, des mots de passe d'administrateur inscrits dans le code et le passage d'un fournisseur compromis à ses clients via les relations de confiance.

L'enjeu, pour le FBI et le CERT-EU, n'est pas une nouvelle faille mais la vitesse : un petit groupe peu compétent peut mener plusieurs intrusions à la fois et achever l'attaque avant que les défenseurs ne réagissent, même si le trafic généré est bruyant et peut déclencher des alertes.

Pourquoi on en parle

C'est l'un des premiers cas documentés par les autorités de plusieurs pays où un agent d'IA accessible à tous est utilisé à grande échelle pour de vraies attaques, et le premier qui touche directement la Commission européenne. Pour les organisations, l'échelle de temps change : les failles connues mais non corrigées et les systèmes oubliés sur internet sont trouvés et exploités en quelques heures, pas en semaines.

L'affaire relance aussi le débat sur les outils à double usage : ARTEX est né pour des tests autorisés, et le même type d'automatisation aide les défenseurs à trouver leurs propres faiblesses en premier. C'est pourquoi le CERT-EU

recommande de surveiller l'usage des outils d'IA sur son propre réseau et de ne pas laisser en suspens les failles jugées mineures.

Ce que disent les règles

Les actes de la base qui concernent la sécurité des institutions de l'UE, les systèmes d'IA et la gestion du risque cyber.

Règlement (UE, Euratom) 2023/2841 établissant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans les institutions, organes et organismes de l'Union

Le règlement sur la cybersécurité des institutions, organes et organismes de l'Union : il impose à chacun des mesures de gestion des risques et la notification des incidents importants au CERT-EU, qui leur sert de service commun. C'est le cadre de l'attaque contre la Commission et de l'alerte du CERT-EU.

Directive (UE) 2022/2555 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union (directive SRI 2)

Pour les entreprises et organismes des secteurs essentiels et importants, NIS 2 exige la gestion des vulnérabilités, la sécurité de la chaîne d'approvisionnement et la notification rapide des incidents (art. 21 et 23) : les mesures qu'ARTEX met à l'épreuve, avec des attaques qui durent quelques heures.

Règlement (UE) 2024/1689 établissant des règles harmonisées concernant l'intelligence artificielle (règlement sur l'intelligence artificielle)

Le règlement sur l'intelligence artificielle impose aux fournisseurs de modèles d'IA à usage général présentant un risque systémique d'évaluer et d'atténuer les risques systémiques et de garantir un niveau de cybersécurité adéquat (art. 55) ; parmi les risques systémiques, le considérant 110 cite les capacités cyber offensives, comme la découverte et l'exploitation des vulnérabilités. L'affaire montre pourquoi ils comptent.

Les normes de référence

Les normes de la base les plus utiles pour réduire la surface d'attaque et encadrer l'usage de l'IA.

CIS Controls v8.1 – Contrôles de sécurité critiques du CIS

Les contrôles 1 et 2 (inventaire des actifs et des logiciels), 7 (gestion continue des vulnérabilités) et 12 (gestion de l'infrastructure réseau) sont la première défense contre un outil qui cherche justement les systèmes oubliés.

OWASP Top 10:2025 – OWASP Top 10:2025 – Les dix risques de sécurité les plus critiques pour les applications web

Les failles exploitées par ARTEX selon le FBI (contrôle d'accès, mauvaises configurations, SSRF, identifiants dans le code) sont des catégories de l'OWASP Top 10 : une liste à utiliser pour contrôler les portails et applications web exposés.

NIST CSF 2.0 – Cadre de cybersécurité du NIST (CSF) 2.0

Le cadre pour organiser la défense : inventaire et gestion des fournisseurs (Govern et Identify), protection des accès, détection et réponse rapides (Detect et Respond), qui doivent être prêtes quand les attaques durent quelques heures.

NIST AI RMF 1.0 – Cadre de gestion des risques liés à l'intelligence artificielle (AI RMF 1.0)

Le cadre du NIST pour gérer les risques des systèmes d'IA : utile à qui développe ou utilise des agents d'IA, y compris pour les tests de sécurité, pour définir les usages admis, les contrôles et les responsabilités.

ISO/IEC 42001:2023 – Technologies de l'information – Intelligence artificielle – Système de management

Le système de management de l'IA : des règles internes sur les outils d'IA autorisés, par qui et avec quels contrôles, comme le demande le CERT-EU lorsqu'il recommande de surveiller l'usage de l'IA sur son propre réseau.

Sources de l'analyse

1. **Sources officielles:** Federal Bureau of Investigation (FBI), FLASH-20261113-001 – Threat Overview of ARTEX Autonomous Penetration Testing Framework ↗, 13 novembre 2026.https://www.ic3.gov/csa/2026/261113.pdf
2. CERT-EU, From Penetration Testing to Cyber Threat: Beware of ARTEX ↗, 5 novembre 2026.https://cert.europa.eu/blog/from-penetration-testing-to-cyber-threat-beware-of-artex

3. National Cyber Security Centre (NCSC), Switzerland, Cyberattacks involving AI agents: First confirmed cases in Switzerland ↗, 24 novembre 2026.https://www.bacs.admin.ch/en/26-ki-agenten-1-en
4. Bundesamt für Sicherheit in der Informationstechnik (BSI), Hoher Reifegrad von Agentic Offensive Frameworks verschärft Bedrohungslage ↗, 26 novembre 2026.https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KI/Offensive-agentische-KI_261115.html
5. European Commission – Audiovisual Service, EC Midday press briefing of 19/11/2026 – Cybersecurity: Cyber campaign against the European Commission, Q&A ↗, 19 novembre 2026.https://audiovisual.ec.europa.eu/en/media/video/I-298222
6. European Commission – Audiovisual Service, EC Midday press briefing of 23/11/2026 – Cybersecurity: Cyber campaign against the European Commission, Q&A ↗, 23 novembre 2026.https://audiovisual.ec.europa.eu/en/media/video/I-298395
7. **Presse:** The Record (Recorded Future News), European Commission confirms cyberattack, says hackers used AI tool ↗, 19 novembre 2026.https://therecord.media/european-commission-confirms-cyberattack-using-ai

Pour une réponse pratique

- Qui notifier et dans quel délai en cas d'incident, pays par pays
- Les autorités nationales et les CSIRT de chaque pays
- La page de votre secteur : lois de l'UE, actes spécifiques et normes

Sources et données

Point « ce que l'on sait » fondé sur l'alerte FLASH du FBI, sur l'analyse du CERT-EU, sur les déclarations du porte-parole de la Commission européenne aux briefings de midi des 19 et 23 novembre et, lorsque c'est indiqué, sur des médias. Il vaut pour les faits connus à la date indiquée. Les sources citées font foi.

- Page interactive: SRI 2 https://www.cybersecuritydatabase.org/fr/transposition/nis2/
- Page interactive: REC https://www.cybersecuritydatabase.org/fr/transposition/cer/
- Page interactive: Normes et cadres https://www.cybersecuritydatabase.org/fr/standards/
- Données ouvertes (JSON): documents.json https://www.cybersecuritydatabase.org/api/v1/documents.json

Comment citer

Cybersecurity Database, « ARTEX, l'outil d'attaque piloté par l'intelligence artificielle signalé par le FBI et le CERT-EU (2026) », données au 27 novembre 2026, https://www.cybersecuritydatabase.org/fr/reports/artex-ai-hacking-tool/. Licence CC BY 4.0.