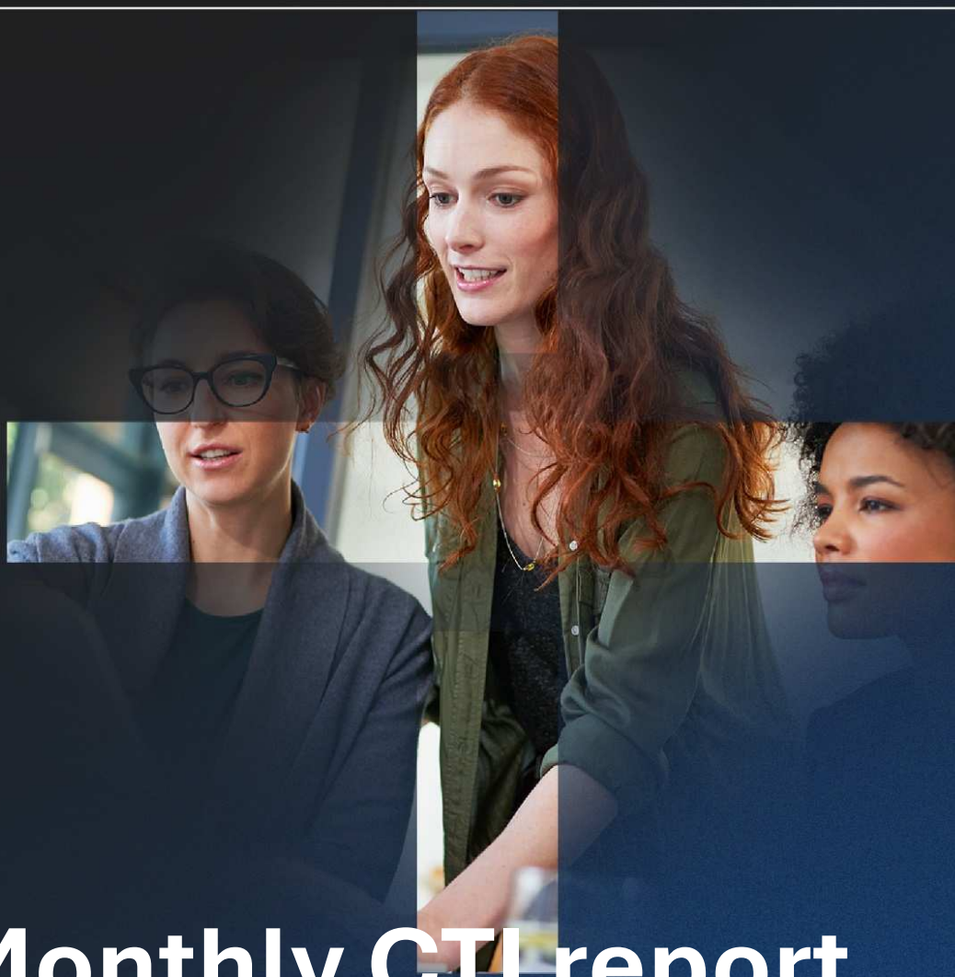
aDvens

For cyber, people & planet



Monthly CTI report

March 2026

CERT aDvens - CTI
Advens - 38 rue des Jeuneurs - 75002 Paris

TABLE OF CONTENT

1. Executive summary . . . 2
2. Vulnerabilities . . . 3
2.1. CVE-2026-33309 - Langflow . . . 3
2.1.1. Risk . . . 3
2.1.2. Type of vulnerability . . . 3
2.1.3. Severity (base score CVSS 3.1) . . . 3
2.1.4. Impacted product . . . 4
2.1.5. Recommendation . . . 4
2.1.6. Proof of concept . . . 4
2.2. CVE-2026-3564 - ScreenConnect . . . 5
2.2.1. Risk . . . 5
2.2.2. Type of vulnerability . . . 5
2.2.3. Severity (base score CVSS 3.1) . . . 5
2.2.4. Impacted product . . . 5
2.2.5. Recommendation . . . 5
2.2.6. Proof of concept . . . 5
2.3. CVE-2026-23489 - GLPI . . . 6
2.3.1. Risk . . . 6
2.3.2. Type of vulnerability . . . 6
2.3.3. Severity (base score CVSS 3.1) . . . 6
2.3.4. Impacted product . . . 6
2.3.5. Recommandation . . . 6
2.3.6. Proof of concept . . . 6
3. Geopolitical Hacktivism in Europe: DDoS, Wipers, and Domino Effect on the Supply Chain since February 2026 . . . 7
3.1. Coordinated DDoS Reactions in Retaliation for Pro-Ukraine European Policy Decisions . . . 7
3.2. Destructive attacks with a ripple effect on European healthcare systems: the pro-Iranian response to the US and Israeli strikes . . . 10
3.3. Conclusion: The Supply Chain as the main vector of Domino Effects in Europe . . . 11
3.4. Recommendations . . . 12
4. Sources . . . 13

1. EXECUTIVE SUMMARY

This month, CERT aDvens brings you an overview of emerging threats and recently identified vulnerabilities:

- Three new security vulnerabilities have been detected, one of which has a public *proof of concept* (PoC). These add to the vulnerabilities previously identified.
- An analysis of recent hacktivist attack campaigns, in the context of the conflicts in Ukraine and Iran.

These topics aim to help you anticipate risks and strengthen your cybersecurity posture.

2. VULNERABILITIES

This month, the CERT aDvens highlights three vulnerabilities affecting commonly used technologies within companies.
They are sorted by severity (proofs of concept available, exploitation...). Applying their patches or workarounds is highly recommended.

2.1. CVE-2026-33309 - Langflow

CVE-2026-33309 provides an additional fix to the one for CVE-2026-68478 in Langflow-AI, which was incomplete. Langflow is a tool for creating and deploying AI-based agents and workflows.

A path traversal vulnerability in LangFlow *POST /api/v2/files/* endpoint allows an authenticated attacker to execute arbitrary code by sending specially crafted requests.

This vulnerability was disclosed in a security bulletin on the 24 March 2026, with a proof-of-concept provided by the Langflow-AI developers. On the 17 March 2026, they had also published a proof-of-concept in the CVE-2026-33017 advisory. **This was exploited twenty hours later**.

2.1.1. Risk

- Remote code execution

2.1.2. Type of vulnerability

- **CWE-22**: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
- **CWE-73**: External Control of File Name or Path
- **CWE-94**: Improper Control of Generation of Code ('Code Injection')
- **CWE-284**: Improper Access Control

2.1.3. Severity (base score CVSS 3.1)

Attack vector	Network	Scope	Changed
Attack complexity	Low	Impact on confidentiality	High
Privileges Required	Low	Impact on integrity	High
User Interaction	None	Impact on availability	High

2.1.4. Impacted product

Langflow :

- Version 1.2.0 and later
- Version 1.8.1 and prior

2.1.5. Recommendation

Update Langflow to version 1.9.0 or later.

Additional information are available in the Langflow-AI's advisory.

2.1.6. Proof of concept

To date, a proof of concept is available in open sources.

2.2. CVE-2026-3564 - ScreenConnect

CVE-2026-3564 is a vulnerability affecting ScreenConnect. This remote access platform is widely used by managed service providers, IT departments, and technology solution providers.

An improper validation of ASP.NET cryptographic signatures in ScreenConnect allows an unauthenticated attacker, by extracting these keys from configuration files, to bypass the session authentication process.

ScreenConnect is used for managing remote devices, so attackers can log in remotely to employees' computers, execute commands, or install malware.

2.2.1. Risk

- Security policy bypass

2.2.2. Type of vulnerability

- **CWE-347**: Improper Verification of Cryptographic Signature

2.2.3. Severity (base score CVSS 3.1)

Attack vector	Network	Scope	Changed
Attack complexity	High	Impact on confidentiality	High
Privileges Required	None	Impact on integrity	High
User Interaction	None	Impact on availability	High

2.2.4. Impacted product

- ScreenConnect versions prior to 26.1

2.2.5. Recommendation

Update ScreenConnect to version 26.1 or later.

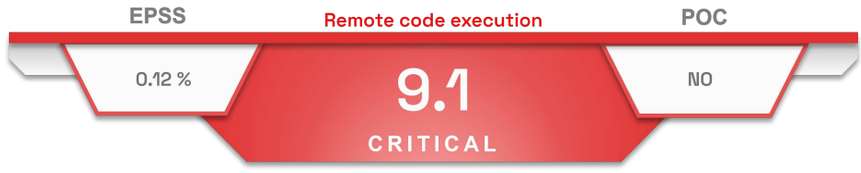
Additional information is available in the ConnectWise's advisory.

2.2.6. Proof of concept

To date, no proof of concept is available in open sources.

2.3. CVE-2026-23489 - GLPI

The vulnerability CVE-2026-23489 was disclosed on the 16 March 2026 and affects the Fields plugin in GLPI, which allows users to add custom fields to objects such as tickets, computers, or users, that are not included by default.



An improper of validation of user-provided data in the GLPI Fields plugin allows an attacker authenticated as an authorized user to create drop-down lists and execute arbitrary PHP code on the GLPI server.

GLPI is an open-source IT service management software solution designed to track hardware and user requests. It is widely used in government agencies and certain critical infrastructure operators, such as hospitals.

2.3.1. Risk

- Remote code execution

2.3.2. Type of vulnerability

- **CWE-20**: Improper Input Validation

2.3.3. Severity (base score CVSS 3.1)

Attack vector	Network	Scope	Changed
Attack complexity	Low	Impact on confidentiality	High
Privileges Required	High	Impact on integrity	High
User Interaction	None	Impact on availability	High

2.3.4. Impacted product

Fields plugin for GLPI version 1.23.2 and prior

2.3.5. Recommandation

Update the Fields plugin in GLPI to version 1.23.3 or later.

Additional information is available in the GLPI's bulletin.

2.3.6. Proof of concept

To date, no proof of concept is available in open sources.

3. GEOPOLITICAL HACKTIVISM IN EUROPE: DDOS, WIPERS, AND DOMINO EFFECT ON THE SUPPLY CHAIN SINCE FEBRUARY 2026

Since the beginning of March 2026, the European continent has experienced a significant increase of the hacktivist threat, resulting from both the military escalation in the Middle East and European political choices in favor of Ukraine. This has led to a wave of protests from cybercriminal actors. Data consolidated by Radware shows that, in the seventy-two hours following the US-Israeli strikes of February 28, 2026, while the majority of attacks targeted the Middle East (Israel, Kuwait, Jordan), Europe nevertheless absorbed nearly 23% of global attacks. This figure confirms that the European territory remains a secondary, but structuring, theater of hacktivist attacks. Two dynamics can explain the rise in hacktivist actions: **a phenomenon of protest against European policy decisions related to the Ukrainian conflict** and **the military escalation between the United States, Israel, and Iran**. This analysis focuses on attacks that took place between the 1st and the 26th of March 2026.

3.1. Coordinated DDoS Reactions in Retaliation for Pro-Ukraine European Policy Decisions

Europe is the target of retaliatory campaigns led primarily by NoName057(16) after any government decision perceived as strengthening support for Ukraine. This **retaliation-driven DDoS model** consists of publicly punishing the state in question with saturation attacks directed against its government portals, administrative infrastructure, transportation systems, energy services, or judicial platforms. The goal is to render them temporarily unavailable to signal displeasure. Throughout March, Germany, as well as Cyprus, Denmark, Spain, Finland, Romania, and Ukraine, were targeted. In each case, the country was chosen as the attack target following a political decision.

Thus, on the 25th of February 2026, the fourth anniversary of the invasion of Ukraine, the Bundestag adopted a resolution strengthening German military aid and tightening European sanctions. In the days that followed, NoName057(16) immediately refocused its activity on Germany, which became the primary target of a series of DDoS attacks. Thirty-seven attacks were claimed on the group's Telegram channel between the 1st and the 26th of March 2026.

Figure 1. NoName057(16) explains on the 2nd of March 2026 the reason why the group is targeting Germany (source Telegram)

The same pattern repeated itself in Romania on March 12, 2026, during the Ukrainian president's visit to Bucharest. A bilateral military cooperation agreement providing for the joint production of drones in Romania was signed, triggering a wave of DDoS attacks from NoNameO57(16) against the country, with 25 attacks recorded in six days.

Figure 2. NoName057(16) explains on the 16th of March 2026 the reasons why the group is targeting Romania (source Telegram)

Furthermore, following several announcements published in February in the European press regarding the growing role of Cyprus and Denmark in supplying military equipment to Ukraine, NoName057(16) actively targeted these two countries in March (30 attacks for Cyprus and 14 for Denmark). The hacktivist group disputes the role of Denmark, which, along with Sweden, provides Kyiv with H-10 Poseidon drones, and of Cyprus, which produces TRIDON Mk2 anti-aircraft systems. The targeting of Denmark was also motivated by the signing of a bilateral agreement between Denmark and Ukraine on February 23, 2026, for €1.8 billion in military and capability support. The country was then inundated with dozens of claims of responsibility for attacks: government agencies, public services, transport operators, and government portals were targeted, with a notable intensification on the 26th and 27th of February. These attacks continued throughout March. Other pro-Russian groups, such as DarkStorm, also took part in the conflict, putting pressure on other Danish victims, including Bornholm Airport, on the 24th of March 2026.

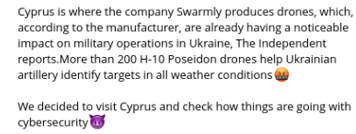


Figure 3. Publication by NoName057(16) - targeting Cyprus - 9th of March 2026 (source: Telegram)

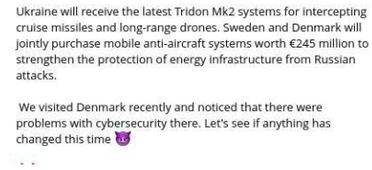


Figure 4. Publication by NoName057(16) - targeting Danemark - 23rd of March 2026 (source Telegram)

Two distinct spikes are observed on the 1st and the 5th of March. These concern attacks on Germany following statements by NoName057(16) regarding Berlin's political decisions. The same is true for the spikes on the 11th of March and the of March 16th-18th, which are respectively linked to attacks on Cyprus and Romania by NoName057(16) after announcements on its Telegram channel. The intermediate fluctuations are linked to sporadic attacks on Denmark, Cyprus, Ukraine, Spain, and Finland.

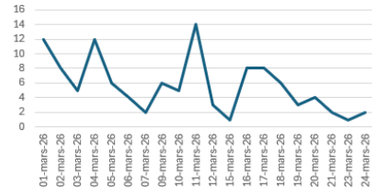


Figure 5. Timeline - spikes in hacktivist group attacks in response to political decisions (source: CERT ADVENS)

Thus, **Europe is under hacktivist pressure in response to its own political decisions**: the Bundestag vote, the Denmark-Ukraine agreement, strategic announcements, etc. Between the 1st anf the 26th of March 2026, CERT Advens identified 119 European entities as victims of massive DDoS attacks. Seven countries were targeted (see graph below). The most targeted country was Germany with 37 claimed attacks, followed by Cyprus (30) and Romania (25). Government institutions were the primary targets, accounting for more than half of the DDoS attacks, followed by the transport sector (13 attacks), finance (11 attacks), industry/aerospace (11 attacks), energy (8 attacks), and media (7 attacks). French companies could also be targeted in retaliation for government action by the Élysée Palace in the Ukrainian conflict.

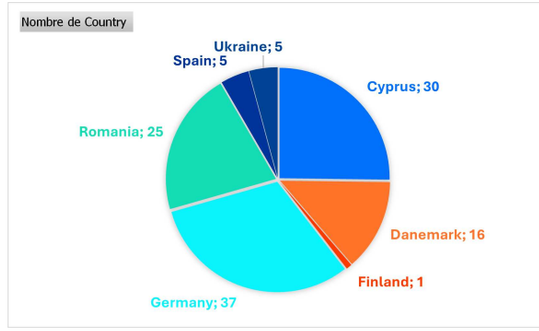


Figure 6. European countries targeted between the 1st and the 26th of March 2026 (source: CERT Advens)

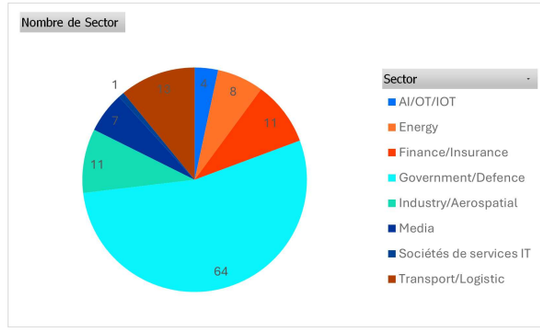


Figure 7. Targeted sectors in Europe between the 1st and the 26th of March 2026 (source: CERT Advens)

3.2. Destructive attacks with a ripple effect on European healthcare systems: the pro-Iranian response to the US and Israeli strikes

Alongside pro-Russian campaigns targeting Europe, **the military escalation in the Middle East has triggered the emergence of groups aligned with Iranian interests, including Handala**, a unit operating under the authority of the Iranian Ministry of Intelligence and Security (MOIS). On the night of the 11th of March 2026, the Handala group attacked the American medical technology giant Stryker in retaliation for the strike of 28th February 2026 on a school in Minab that killed more than 70 people. More than 200,000 devices were remotely wiped in 79 countries, compromising Stryker's business continuity and, through a ripple effect, impacting the healthcare sector in Europe. The group claims to have exfiltrated 50 terabytes of data. The attack against Stryker is the pro-Iranian counterpart to what we see on the pro-Russian side with NoName057(16).

The Handala group is a pro-Palestinian hacktivist group that formed in the wake of the attacks of 7 October 2023. The US Department of Justice and several other agencies assess with a high degree of confidence that this group is a front linked to the Red Sandstorm unit, enabling the Iranian regime to carry out attacks whilst maintaining plausible deniability. The group has Starlink equipment enabling it to circumvent Iranian power cuts, controls several portals and infrastructure, and demonstrates great resilience: every time a site is shut down, it is rebuilt shortly afterwards.

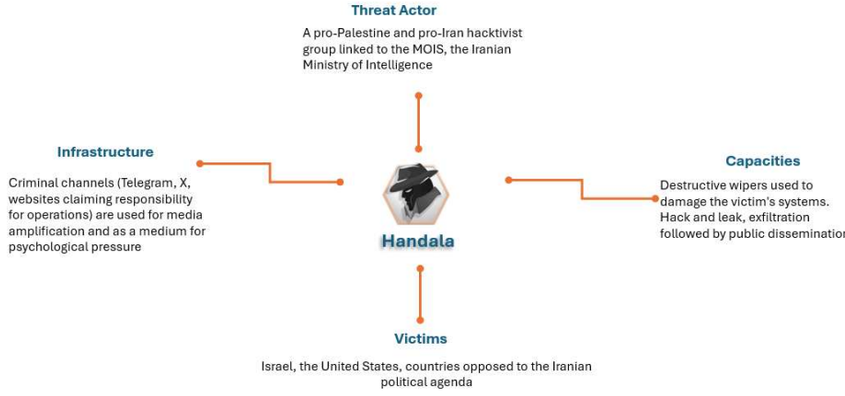


Figure 8. Diamond Model Handala threat actor

Figure 9. Claim of responsibility by the Handala group regarding the Stryker attack (source: Telegram)

Here too, the strategic approach is identical to that of NoName057(16): immediate reaction to a Western military decision, choice of a symbolic but non-military target, claiming responsibility for the attacks through the groups on Telegram, and an explicit desire to demonstrate that Western actions have a cost.

Following the attack on Stryker, the United States did not want to let the Handala group go unpunished. On the 19th of March 2026, the U.S. Department of Justice announced the seizure of four domain names associated with the Handala group. According to the FBI affidavit, the seized domain names included those originally used to claim responsibility for the attack against Stryker. Handala responded to the attack the same day on its Telegram channel and rebuilt its infrastructure to ensure business continuity. Further attacks by the cybercriminal group on the West are conceivable, such as the one on Lockheed Martin on the 26th of March 2026.

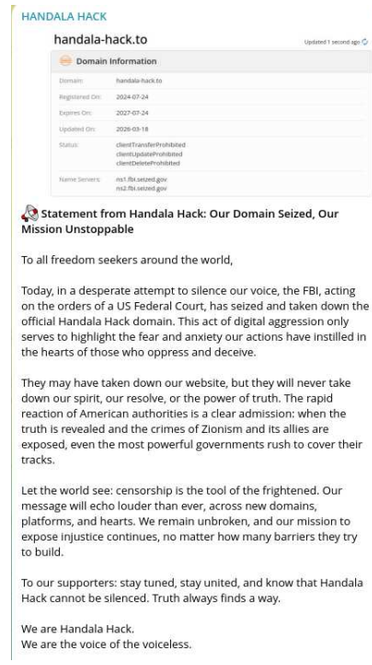


Figure 10. Positioning of the Handala group following the seizing of its domain names (source Telegram)

While pro-Russian attacks primarily target the European Union via DDoS attacks, the Stryker attack demonstrates that the Iranian response aims to disrupt the operational continuity of Western multinationals, resulting in an indirect but potentially critical impact on European healthcare systems. On both fronts, —pro-Russian and pro-Iranian—hacktivist groups are using institutions and businesses as levers of geopolitical pressure.

3.3. Conclusion: The Supply Chain as the main vector of Domino Effects in Europe

The events of February and March 2026 demonstrate that the hacktivist threat in Europe is no longer limited to direct attacks against governments or national infrastructure. The Stryker episode reveals a major strategic reality: Europe's systemic vulnerability to its global industrial, logistical, and technological dependencies. By targeting an American multinational deeply integrated into European hospital ecosystems, pro-Iranian actors caused significant collateral damage in Europe without ever directly attacking its institutions.

This domino effect highlights an evolution in geopolitical hacktivism:

- Pro-Russian DDoS attacks are a response to European political decisions (aid to Ukraine, bilateral agreements, parliamentary resolutions),
- Pro-Iranian destructive attacks are a response to Western military actions (strikes in the Middle East).

In both cases, it is not the activities of European states themselves that motivate the attacks, but their geopolitical positioning. This creates a context in which European companies—including French ones—can be targeted without initial intent, simply because they belong to a supply chain perceived as Western or aligned with a strategic camp.

Thus, France, even without being directly targeted, can be affected through its technological, medical, or logistical dependencies, within the framework of geopolitical crises that it did not initiate, but to which it is intrinsically linked. French companies can therefore be targeted across their supply chain as a consequence of hacktivist campaigns rooting from the diplomatic decisions of their own government.

3.4. Recommendations

To limit the risks of a DDoS attack and reduce its immediate impact, several measures should be implemented:

- Establish a cyber threat monitoring and intelligence system tailored to hacktivism (monitoring of ANSSI, ENISA, etc.)
- Regularly assess the geopolitical risk profile to identify exposures linked to partnerships, sectors of activity (transport, energy, finance, healthcare, international events) or third-party suppliers.
- Implement dynamic and contextual filtering: temporary IP or geographical blocking based on real-time intelligence, granular rate limiting per endpoint or API, adaptive CAPTCHA or JavaScript challenges.
- Configure a web application firewall (WAF) with behavioural rules based on machine learning, anomaly detection (known DDoSia patterns, traffic entropy) and advanced bot management.
- Ensure infrastructure redundancy via multiple CDNs, geographical zones and auto-scaling mechanisms.
- Conduct regular DDoS simulations to validate the effectiveness of the entire system.
- Protect APIs and web services via a dedicated gateway with rate limiting and strong authentication. Deploy a behavioural monitoring system (SIEM with UEBA and machine learning) to identify abnormal spikes before complete saturation.
- Integrate EDR/XDR solutions on endpoints and Network Detection and Response (NDR) tools to detect reconnaissance phases or botnet activity.
- Set up 24/7 monitoring via a SOC (in-house or outsourced), with alert thresholds specific to hacktivist campaigns (traffic originating from high-risk areas via known proxies or VPNs).
- Draft a dedicated DDoS playbook to specify rapid escalation to a crisis response team, communication procedures (internal, clients, media, authorities such as ANSSI) and coordination with suppliers and ISPs.
- Conduct simulation exercises (tabletop and live tests) quarterly to validate the plan.
- Plan a fallback mode for critical services (static fallback, asynchronous queues, offline mirrors) with appropriate RTO/RPO targets.
- Create a detailed map of dependencies and a three-tier prioritisation (critical, important, support) to guide decision-making in a crisis.
- Adopt Zero Trust principles (micro-segmentation, least privilege access, continuous monitoring) to mitigate risks where a DDoS attack serves as a cover for a deeper intrusion.
- Assess the digital supply chain and impose stricter requirements on third-party providers (CDNs, hosting providers, SaaS) regarding their DDoS resilience.
- Train staff to recognise phishing or spear-phishing attempts, which often precede DDoS campaigns, as well as the risks associated with insider threats.
- Conduct regular penetration tests and red teaming exercises incorporating geopolitical hacktivist scenarios.

4. SOURCES

CVE-2026-3564 - ScreenConnect :

- https://nvd.nist.gov/vuln/detail/CVE-2026-3564
- https://www.connectwise.com/company/trust/security-bulletins/2026-03-17-screenconnect-bulletin
- https://www.helpnetsecurity.com/2026/03/20/connectwise-screenconnect-cve-2026-3564/
- https://darknetsearch.com/knowledge/news/en/screenconnect-vulnerability-7-key-risks-revealed/

CVE-2026-33309 - Langflow-AI :

- https://nvd.nist.gov/vuln/detail/CVE-2026-33309
- https://github.com/langflow-ai/langflow/security/advisories/GHSA-g2j9-7rj2-gm6c
- https://www.cisa.gov/news-events/alerts/2026/03/25/cisa-adds-one-known-exploited-vulnerability-catalog
- https://www.helpnetsecurity.com/2026/03/27/cve-2026-33017-cve-2026-33634-exploited/
- https://thehackernews.com/2026/03/langchain-langgraph-flaws-expose-files.html

CVE-2026-23489 - GLPI :

- https://nvd.nist.gov/vuln/detail/CVE-2026-23489
- https://github.com/pluginsGLPI/fields/releases/tag/1.23.3
- https://github.com/pluginsGLPI/fields/security/advisories/GHSA-rj7q-mmx9-fhq7
- https://fr.linkedin.com/posts/login-s-curit-_glpi-activity-7440306708968656897-vGVI

149 Hacktivist DDoS Attacks Hit 110 Organizations in 16 Countries After Middle East Conflict https://thehackernews.com/2026/03/149-hacktivist-ddos-attacks-hit-110.html