ARMIS®

LABS

INSIGHTS

# Catch Attackers Before They Strike

Early Warning Insights for the **Financial Services Industry**

# What Makes Armis Labs Different?

Armis Labs' proactive threat detection capabilities enable organizations to stay one step ahead of cyber adversaries, minimizing the risk of potential breaches while stopping potential damage before it occurs.

**3800+**

Armis Centrix™ for Early Warning is currently tracking over **3800 CVEs that are not published on CISA's Known Exploited Vulnerabilities (KEV) Catalog.**

# Why Does This Matter?

**28%**

Once a vulnerability is published on CISA KEV, around **28% are exploited same-day.** This highlights the value of Early Warning insights and the need to patch quickly.

# Executive Summary

The global financial services sector is presently navigating a cyber landscape defined by complexity, speed, and systemic interdependence. Digital infrastructure, which forms the foundation of global economies, has intensified into a continuous, high-stakes battleground where traditional defenses are increasingly challenged by sophisticated, digital adversaries.

## Armis Labs Findings:

**63%** 63% of exploits in Financial Services originate from hardware or software manufacturers, amplifying their impact. Zero-days like CVE-2024-50623/55956 affected 389 victims in Q1 2025 alone.

**40%** 40% of attacks used vulnerabilities as a beachhead to gain entrance into a secured environment, up from 14% in 2023. Endpoint device flaws topped Q2 2025 lists, with the Qilin cybercrime group claiming 101 incidents.

**65%** In Financial Services, 65% of attacks hit via unpatched assets, with an average $2.73M recovery cost.

While spending on security in the sector reached $215 billion in 2024, reflecting a robust 14.3% increase from the previous year (source), this paradox of massive investment alongside protracted detection times suggests that current Cybersecurity budget allocation areas may be failing to address foundational defensive weaknesses.

This necessitates a strategic pivot toward intelligent Cyber Exposure Management (CEM) and proactive incident response capabilities. Financial institutions need to look beyond simple compliance and address the underlying causality of risk, including:

- **A “left of boom” approach to Cyber Exposure Management,** with preemptive, early warning strategies, which emphasize proactive measures to identify and neutralize threats before they can inflict damage.
- **Faster securing, testing and remediation** because of supply chain attacks, and endpoint and network devices compromise.
- **A more comprehensive approach to threats** - instead of mainly SIEM-based using TTPs to numerous security products, including Intrusion Prevention Systems (IPS), Web Application Firewalls (WAF), Endpoint Detection and Response (EDR), etc. Organizations must seek greater value of existing security products.

- **Qualitative Investment Shifts** to prioritize intelligence-driven and collaborative security (e.g., AI-based threat detection tools) that measurably reduces attacker dwell time, rather than merely increasing total security spend.
- **Governance Hardening** to implement mandatory governance and security controls and employee/partner training programs, and counteract AI-driven identity fraud that targets the veracity of internal decision-making.

Research for this report was conducted in Q4, 2025 by Armis Labs security practitioners, utilizing cutting edge technology that include deception technologies, incident forensics, reverse engineering, dark web monitoring, and human intelligence to proactively identify and mitigate threats before they manifest.

# The Weaponization of GenAI

AI has become a primary force multiplying the effectiveness of criminal enterprises. This is particularly evident in the deployment of digital deception. GenAI and Agentic AI are enabling highly sophisticated attacks that target the human element and undermine the governance structures of financial institutions.

## Deepfake Executive Fraud

Malicious actors are cloning the voices and appearances of executives during live video calls to deceive high-value employees into transferring substantial funds. This attack vector is an AI-enhanced evolution of traditional Business Email Compromise (BEC) and poses a severe threat to internal governance, as it attacks the root of corporate decision-making authority. In the financial sector, deepfake incidents result in high financial losses, averaging over $600,000 per incident (source). These synthetic replicas are capable of bypassing critical operational security controls, including Know Your Customer (KYC) and Anti-Money Laundering (AML) checks, by deceptively manipulating verification systems.

## Sophisticated Social Engineering Attacks

Traditional spear phishing required manual research and customization; however, malicious AI agents can now autonomously harvest data from social media profiles, craft grammatically flawless, highly personalized phishing and spear phishing messages, and launch thousands of tailored attacks simultaneously. This capability eliminates commonly known warning signs, such as poor grammar, making the attacks difficult to detect and diminishing the effectiveness of traditional cybersecurity training.

## Speed of Vulnerability to Exploitation

GenAI significantly accelerates the speed of vulnerability exploitation by drastically reducing the time and skill required for threat actors to move from vulnerability discovery to a working exploit. This is often referred to as “weaponization time” or the shrinking of the “window of exposure.” The speed of both attack and defense is escalating, making the window of time an organization has to patch a vulnerability critically short.

## Adaptive Malware

GenAI tools are being leveraged to develop and pilot more sophisticated malware, granting complex attack capabilities to a broader range of threat actors. AI allows this malicious code to adapt dynamically, evading real-time detection by traditional signature-based intrusion detection systems. This technological sophistication demands that financial institutions move beyond static defenses toward intelligent, predictive security mechanisms.

# FinTech, Interconnectedness, and Concentration Risk

FinTech represents a dual-edged sword for financial stability. While it drives innovation, financial inclusion, and service efficiency through technologies like blockchain and artificial intelligence, it simultaneously introduces new, faster risk transmission channels and cybersecurity vulnerabilities.

## Interconnectedness

When institutions are highly dependent on each other, particularly through shared services, or hold overlapping portfolios, security events that impact one institution are more likely to spread rapidly to others. FinTech exacerbates this by creating asymmetries in trust and control, especially when institutions rely heavily on third-party platforms.

This is particularly critical in emerging economies, where rapid FinTech adoption often surpasses the pace at which corresponding risk management frameworks are developed, allowing systemic risks to escalate unchecked.

The high speed and automated nature of FinTech platforms mean that a cyber failure, such as API exploitation or large-scale data theft, can trigger financial or reputational shocks much faster and across more integrated entities than traditional banking contagion models predicted. Thus, FinTech cyber risk must be regarded as an operational risk with immediate liquidity and market implications.

The reliance on APIs is a major vector for security vulnerabilities within the FinTech ecosystem. APIs facilitate the seamless, automated exchange of sensitive data, which is a key component of open banking frameworks, particularly in the EU. However, if not secured properly, these APIs can become exposed entry points, allowing attackers to exploit loopholes, gain unauthorized access to sensitive financial data, or manipulate transactions.

## Cloud Concentration Risk (CCR)

The increasing adoption of cloud services introduces a critical vulnerability known as Cloud Concentration Risk (CCR). This systemic risk arises when a significant portion of the financial sector relies upon a limited number of major technology service providers (e.g., hyperscale cloud providers). In this scenario, a technological disruption or large-scale operational failure at one provider could simultaneously affect the data and systems of numerous financial institutions.

While CCR is a significant regulatory concern, it is not invariably problematic. Regulatory bodies, such as the UK's Prudential Regulation Authority (PRA), recognize that, if correctly configured, cloud services can actually significantly improve the operational resilience of individual firms due to the scale and quality of security offered by major providers. Furthermore, a complex multi-cloud approach, often suggested as a solution to concentration risk, may introduce greater operational risk for many institutions due to added complexity and interconnectedness.

This nuanced view acknowledges that the strategic response must be tailored to specific risks and avoid a one-size-fits-all mandate for multi-sourcing. The global challenge remains: how to secure the core infrastructure used by the sector without stifling the benefits of large-scale cloud adoption.

# Significant Incidents

## Supply Chain and Third-Party Attacks

These attacks exploit the complex, interconnected ecosystem of modern finance, where institutions rely heavily on specialized vendors for core functions, including cloud services, payment processing, software development, and data analytics. Attackers target smaller, less-defended third-party vendors as a means of lateral entry into the primary financial network, effectively bypassing the substantial security investments of major banks.

A successful compromise, such as the injection of malicious code into a widely used software product or the theft of credentials from a managed service provider, can result in simultaneous exposure of sensitive customer data and operational assets across multiple financial institutions, turning a single vulnerability in the supply chain into a systemic threat. A few notable examples include:

**TransUnion**
In August 2025, the credit reporting agency disclosed a breach, part of a wider campaign by the ShinyHunters group targeting third-party applications built on the Salesforce platform. The attack impacted over **4.4 million individuals,** exposing highly sensitive data including full names, dates of birth, and Social Security numbers.

**Santander and DBS Bank**
Both global banks experienced data breaches due to attacks on their respective third-party vendors. Santander's breach through a third-party provider exposed customer data across several countries, while DBS Bank's printing vendor, Toppan Next Tech, was hit by ransomware, potentially compromising statement data for over **8,200 customers.**

**LexisNexis Risk Solutions**
This major data broker experienced a significant breach in May 2025 after an unauthorized party accessed its GitHub account via a third-party software development platform. The incident exposed sensitive personal information for over **364,000 individuals,** including Social Security numbers and driver's license numbers.

**VeriSource Services**
A cyberattack on this benefits and HR administration services provider, disclosed in April 2025, compromised the personal information (including names, addresses, and SSNs) of approximately **4 million individuals** who were clients of their partners.

**Ingram Micro**
The SafePay ransomware group attacked Ingram Micro, a large IT distributor, disrupting global operations and impacting its partners and customers due to a vulnerability in its GlobalProtect VPN.

## Direct Attacks

A critical and evolving shift in direct attacks on Financial Services, is where the very devices designed to be the strongest perimeter defense are becoming the primary initial access vector for sophisticated attacks. The statistic that Edge Security Hardware (firewalls and VPNs) topped the list of exploited vulnerabilities, featuring in 40% of Mandiant's investigations in 2024–2025, underscores a severe systemic risk.

Compromising an edge device often grants the attacker a high level of initial network access and, in some cases, allows them to bypass existing internal segmentation and credential requirements. The spike in brute-force attempts against these devices detected by deceptive technologies in early 2025 confirms a massive, automated effort by cybercriminals to leverage weak credentials or stolen credentials for access.

**FinWise Bank**
In September 2025, an insider breach at FinWise Bank, a platform for FinTech partners, exposed sensitive personal and financial data belonging to about **689,000 customers** of its partner American First Finance.

**Connex Credit Union**
This regional credit union disclosed a breach in August 2025 that affected approximately **172,000 members.** The attack, linked to the ShinyHunters group, exposed sensitive information including names, account numbers, debit card details, and Social Security numbers.

**Coinbase**
In May 2025, the cryptocurrency exchange faced a major extortion attempt stemming from an insider threat: overseas customer support contractors leaked user data. The breach affected over **69,000 users,** compromising names, contact details, and partial Social Security numbers, though no funds were reported stolen.

**Bank Sepah**
The hacker collective "Codebreakers" claimed responsibility for breaching Bank Sepah in March 2025, exfiltrating about 12 TB of data belonging to over **42 million individuals** after the bank refused to pay a ransom.

**Prosper Marketplace**
A cyber attack exposed personal data—including names, Social Security numbers, and income details—of approximately **17.6 million users** due to unauthorized access via compromised administrative credentials, posing significant identity theft risks.

# Top Targets

The previous incidents underscore that all types of financial institutions, from large global banks to smaller credit unions and third-party vendors, remain high-value targets for sophisticated cybercriminals utilizing tactics like ransomware, supply-chain exploitation, and social engineering. Here's an overview of what Armis Labs believes are the current top targets at risk in financial services:

- **Payment Processors and Exchanges**
- **Investment Platforms**
- **Insurance Providers**
- **Crypto Heists**
- **Fintech and Investment Firms**
- **Insurance and Credit Reporting**
- **Bank and Credit Unions**
- **Pension**

# Early Warning Spotlights

**Estimated Organizations Impacted**

**20%**

## Erlang/OTP
## CVE-2025-32433

Customers using Armis Centrix™ for Early Warning were notified about this vulnerability before it appeared in CISA's Known Exploited Vulnerabilities Catalog, enabling them to assess their exposure and act proactively.

| Armis Alert Date | CISA KEV Publish Date | Days Early |
|---|---|---|
| April 19th, 2025 | June 9th, 2025 | 51 |

Erlang/OTP SSH server contains a missing authentication for critical function vulnerability. This could allow an attacker to execute arbitrary commands without valid credentials, potentially leading to unauthenticated remote code execution (RCE). By exploiting a flaw in how SSH protocol messages are handled, a malicious actor could gain unauthorized access to affected systems. This vulnerability could affect various products that implement Erlang/OTP SSH server, including—but not limited to—Cisco, NetApp, and SUSE.

### Understanding The Vulnerability

The vulnerability is severe because it requires no credentials and can compromise affected systems remotely. Patches are provided in OTP-27.3.3, OTP-26.2.5.11, and OTP-25.3.2.20, with a recommended temporary mitigation of disabling the SSH server or restricting access via firewalls until upgrades are applied.

### Remediation

- Upgrade Erlang/OTP to the patched releases: OTP-27.3.3, OTP-26.2.5.11, or OTP-25.3.2.20, depending on your current major/minor branch.
- If immediate upgrade is not feasible, temporarily disable the SSH server or constrain SSH access with firewall rules to prevent unauthenticated connections.
- After upgrading, verify the version is at or beyond the patched releases and re-enable SSH with normal access controls.
- Conduct a security review of SSH exposure (e.g., limit to trusted networks, rotate credentials only if there is evidence of compromise, monitor SSH logs for anomalous activity).
- Run post-patch vulnerability scans and verify that there are no lingering indicators of exploitation.

Estimated Organizations Impacted

**10%**

## Microsoft Office SharePoint
## CVE-2025-49704

Customers using Armis Centrix™ for Early Warning were notified about this vulnerability before it appeared in CISA's Known Exploited Vulnerabilities Catalog, enabling them to assess their exposure and act proactively.

| Armis Alert Date | CISA KEV Publish Date | Days Early |
|---|---|---|
| July 21st, 2025 | July 22nd, 2025 | 1 |

Microsoft SharePoint contains a code injection vulnerability that could allow an authorized attacker to execute code over a network. This vulnerability could be chained with CVE-2025-49706. CVE-2025-53770 is a patch bypass for CVE-2025-49704, and the updates for CVE-2025-53770 include more robust protection than those for CVE-2025-49704.

## Understanding The Vulnerability

The vulnerability has a CVSS base score of 8.8, indicating a high level of risk, with impacts on confidentiality, integrity, and availability all rated as high. The attack vector is network-based, and the complexity is low, meaning that it can be exploited with minimal effort by an attacker who has low privileges and does not require user interaction.

## Remediation

To mitigate the risks associated with CVE-2025-49704, it is recommended that organizations:

- Regularly check for and apply updates or patches provided by Microsoft for SharePoint to address this vulnerability.
- Review and tighten access controls to limit the number of authorized users who can execute code within SharePoint.
- Implement monitoring and logging to detect any unusual activities that may indicate exploitation attempts.
- Follow security best practices for application development and deployment, including input validation and sanitization to prevent code injection vulnerabilities.

# High Impact and Emerging Risks

Armis Labs leverages data from over 6.5 billion assets through the AI-driven Armis Asset Intelligence Engine, combined with deception technology, incident forensics, reverse engineering, dark web monitoring, and human intelligence. The data we gather helps to identify exploited and emerging CVEs, as well as the dominance and impact of those attacks.

During the second half of 2025 we have identified the following CVEs widely exploited in financial services.

| CVE | Vendor | Criticality | First Intel Hit | Estimated % organizations impacted |
|---|---|---|---|---|
| **CVE-2025-53770** | Microsoft | Critical | 2025-07-18 | 9.93 % |
| **CVE-2024-0012** | Palo Alto | Critical | 2024-11-16 | 9.53% |
| **CVE-2025-21535** | Oracle | Critical | 2025-01-21 | 6.4 % |
| **CVE-2024-26169** | Microsoft | High | 2024-06-11 | 52.13 % |
| **CVE-2024-21762** | Fortinet | Critical | 2024-02-09 | 4 % |
| **CVE-2024-55591** | Fortinet | Critical | 2025-01-17 | 1.93 % |
| **CVE-2025-61882** | Oracle | Critical | 2025-10-06 | 0.5 % |
| **CVE-2024-50623** | Cleo | High | 2024-12-12 | 0.4% |
| **CVE-2024-55956** | Cleo | Critical | 2025-03-12 | 0.4 % |
| **CVE-2024-57726** | SimpleHelp | Critical | 2025-02-09 | 0.13 % |
| **CVE-2024-57727** | SimpleHelp | High | 2025-02-09 | 0.13 % |
| **CVE-2024-57728** | SimpleHelp | High | 2025-02-09 | 0.13 % |
| **CVE-2023-34362** | MoveIt | Critical | 2023-06-01 | 0.06 % |
| **CVE-2024-24919** | CheckPoint | N/A | 2024-05-24 | 0.06 % |
| **CVE-2025-31161** | CrushFTP | Critical | 2025-05-27 | 0.06 % |

# Indicators of Compromise

Below are a few concrete Indicators of Compromise (IOCs) in the financial services industry, and their associated detection strategies. Security professionals can use these IOCs and behaviors to identify the presence of these threats in their environments.

## Interlock Ransomware

Active in 2025, opportunistic targeting including Financial Services. Observed in attacks on North American and European organizations, using credential stealers for lateral movement.

**File IOCs:**

- Credential stealer: cht.exe
- Keylogger: klg.dll
- Keylogger output file: conhost.txt

**Associated stealers:** Lumma Stealer, Berserk Stealer variants. These enable harvesting of banking credentials and online account logins.

---

## ToxicPanda Android Banking Trojan

Active in 2025, targeting Europe: Italy, Portugal, Spain.

**Domain IOCs:**

- d7472ad157[.]lol (potential DGA-related)
- ksicngtw[.]org (fallback C2 domain stored in dom.txt)

Uses overlay attacks to steal credentials from banking apps; expanded campaigns in 2025. Commands include overlay loading for fake login screens on targeted banking apps.

---

## Lumma Stealer

Infostealer, frequently targeting Financial Services in 2025. Malware-as-a-Service targeting credentials, banking info, cookies, and crypto wallets; prominent in Q3 2025 detections.

Commonly dropped in phishing or ransomware chains affecting finance.

**IOCs:**

- Monitor for associated C2 domains and hashes from threat feeds (e.g., via MS-ISAC or ThreatFox).

## SmokeLoader Campaigns

2025, financial-themed lures targeting Ukrainian banks.

Distributed via open directories with lures impersonating major banks (e.g., Raiffeisen Bank, Sense Bank). Used to deploy banking trojans or RATs for credential theft.

**IOCs:**

- Look for financial-themed executable lures in misconfigured servers.

## General Phishing Kit

**Example:** Tycoon 2FA, widely used against Financial Services in 2025. Most prevalent AiTM phishing kit for bypassing MFA in financial accounts.

# Conclusion

The cyber threat landscape for the global financial services sector has reached a critical turning point where advanced technologies are being weaponized to create high-impact, systemic risks. The industry is shifting from managing high-frequency, low-impact incidents to defending against sophisticated, low-frequency, high-impact threats that exploit the deep operational interdependence between financial institutions and their vendors.

## Key Takeaways

**Weaponization of Generative AI:** GenAI is significantly accelerating "weaponization time," allowing attackers to move from vulnerability discovery to exploitation almost instantly. It is also fueling highly sophisticated deepfake executive fraud and autonomous social engineering attacks that bypass traditional security training and governance.

**Third-Party and Supply Chain Vulnerability:** A staggering 63% of exploits in financial services originate from vendors. Attackers are increasingly targeting smaller, less-defended third-party providers as a lateral entry point into major financial networks, turning single vendor vulnerabilities into systemic threats.

**Critical Risk from Edge Security:** Edge hardware, such as firewalls and VPNs, has become a primary initial access vector, featuring in 40% of breach investigations in 2024–2025. Compromising these devices often allows attackers to bypass internal segmentation and authentication requirements.

**High Cost of Unpatched Assets:** Approximately 69% of attacks in the sector hit via unpatched assets, leading to an average recovery cost of $2.73 million. The speed of exploitation is so rapid that 28% of vulnerabilities are exploited on the same day they are published on the CISA KEV catalog.

**FinTech and Cloud Concentration Risk:** The rapid adoption of FinTech and reliance on a limited number of hyperscale cloud providers (Cloud Concentration Risk) have created new, faster channels for risk transmission. A single failure in an API or a disruption at a major cloud provider can now trigger immediate liquidity and market implications across the entire ecosystem.

Despite an increase in security spending, traditional defenses are struggling to keep pace, necessitating a strategic move toward "left of boom" proactive intelligence and automated threat detection to reduce attacker dwell time and protect critical infrastructure.

ARMIS LABS

# About Armis Labs

Armis Labs, a division of Armis, is a team of seasoned security professionals dedicated to staying ahead of the ever-evolving cybersecurity landscape. With a deep understanding of emerging threats and cutting-edge methodologies, Armis Labs empowers organizations with unparalleled visibility and expertise to protect against the threats that matter most, right now.

At the heart of Armis Labs lies a formidable research powerhouse, where experts investigate the latest trends and tactics employed by cyber adversaries. Armed with access to over 6.5 billion profiled assets and state-of-the-art tools and methodologies, the team at Armis Labs conducts in-depth analyses of evolving threats both in the pre-emergence stage and “in the wild” stage of an attack.

Armis Labs security practitioners are utilizing cutting edge technology that include deception technologies, incident forensics, reverse engineering, dark web monitoring, and human intelligence to proactively identify and mitigate threats before they manifest. Leveraging advanced AI/ML technologies, Armis Labs’ proactive threat detection capabilities enable organizations to stay one step ahead of cyber adversaries, minimizing the risk of potential breaches while stopping potential damage before it occurs.

Armis Labs is dedicated to providing organizations with the tools and expertise they need to defend against the threats that matter most, right now. With comprehensive vulnerability intelligence, proactive threat detection capabilities, and seamless integration into existing security workflows, Armis Labs empowers organizations to stay ahead of cyber adversaries and protect their most critical assets.

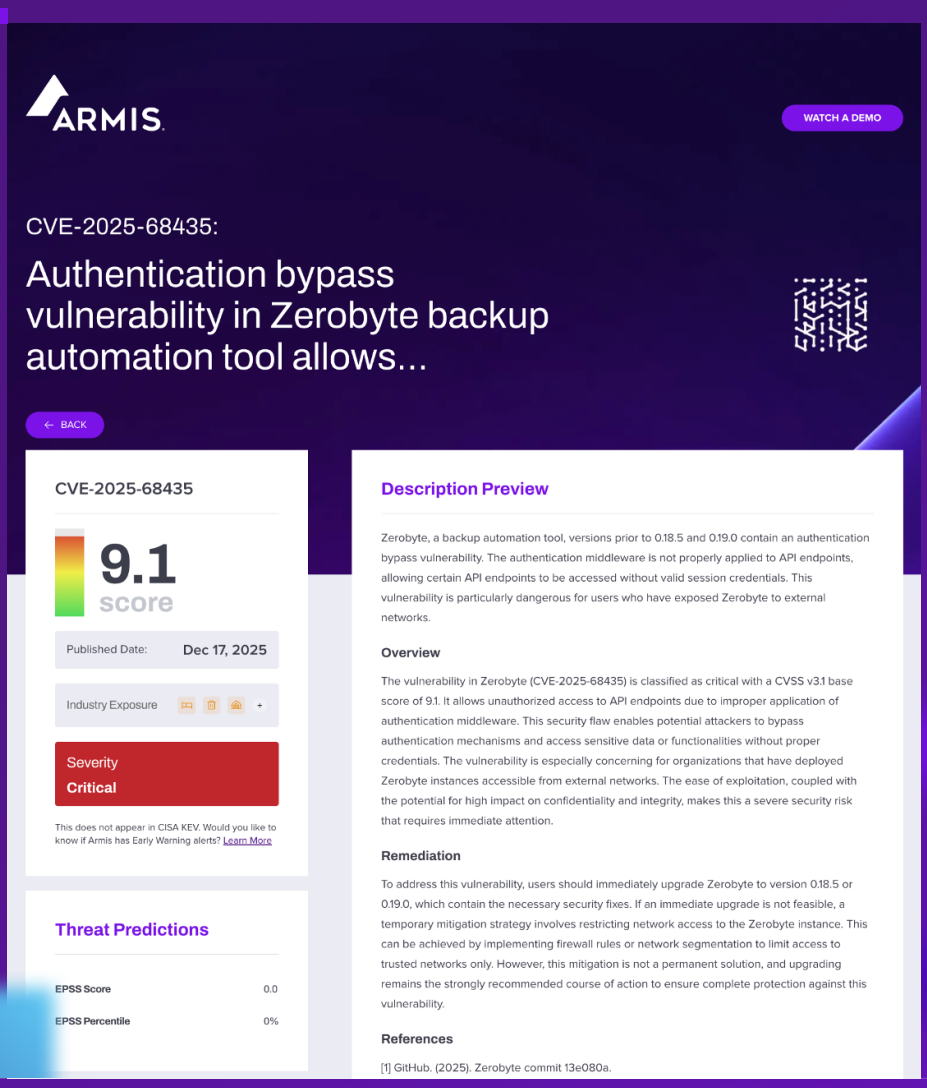
# Ready to Discover More?

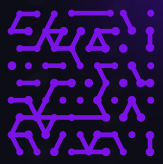
The Armis Vulnerability Intelligence Database is a revolutionary vulnerability intelligence resource that goes well beyond traditional static databases.

While many teams rely on the CISA Known Exploited Vulnerabilities (KEV) catalog to track risk, Armis Vulnerability Intelligence Database is built to extend that value by offering real-time context, extended coverage, and actionable remediation insights tailored to specific industries and threat levels.

Backed by the Armis Asset Intelligence Engine, which observes and analyzes billions of connected assets globally, and Armis Labs, the Armis Vulnerability Intelligence Database offers the cybersecurity community an opportunity to shift left and move from reactive response to proactive risk reduction.

**cve.armis.com**





ARMIS®

**Discover new approaches to protecting your organization - then experience Armis firsthand.**

Experience Armis Centrix™ Live

## Armis, the cyber exposure management & security company, protects the entire attack surface and manages an organization's cyber risk exposure in real time.

In a rapidly evolving, perimeter-less world, Armis ensures that organizations continuously see, protect and manage all critical assets - from the ground to the cloud. Armis secures Fortune 100, 200 and 500 companies as well as national governments, state and local entities to help keep critical infrastructure, economies and society stay safe and secure 24/7.

Armis is a privately held company headquartered in California.

+1 888 452 4011

armis.com