Issue 99 | February 2025

Radar

The cybersecurity magazine

Bank fraud in the digital age: cybersecurity challenges and strategies

By Francisco Javier García Lorente

Bank fraud has evolved from a one-off problem to a global threat affecting both financial institutions and millions of users around the world. Driven by the exponential growth of digital transactions, technological advances and the vulnerability of the human factor, bank fraud represents one of the biggest challenges for modern cybersecurity. This editorial reflects on the challenges associated with this issue and the strategies needed to mitigate its impact.

The evolution of bank fraud

In recent decades, bank fraud has evolved from traditional methods, such as physically stealing cheques or cards, to complex digital tactics designed to exploit both technological and human vulnerabilities. Nowadays, cybercriminals utilise advanced tools such as artificial intelligence, machine learning, and deepfakes to create more sophisticated and personalised attacks.

Among the most common techniques are phishing and its more targeted variant, spear phishing, which are designed to deceive users and steal sensitive credentials. Other notable methods include business email compromise (BEC), where attackers impersonate high-ranking executives to order fraudulent transfers, and ransomware tactics that paralyse banking institutions' systems until a ransom is paid.

This shift in the fraud landscape has transformed the concept of cybersecurity, which no longer solely focuses on protecting networks and systems but now encompasses user education, international regulation, and the adoption of advanced technologies to stay ahead of emerging threats.

Main challenges of cybersecurity against bank fraud

- **Increase in the sophistication of attacks:** Cybercriminals have refined their methods, leveraging artificial intelligence to analyse behavioural patterns and launch more effective attacks. For instance, the use of deepfakes can enable them to bypass biometric systems, while automation tools make it easier to target multiple victims simultaneously.
- **The human factor:** Despite technological advancements, human error remains one of the most vulnerable points. Weak passwords, clicking on malicious links, and a lack of awareness about social engineering tactics allow attackers to compromise systems that would otherwise be secure.
- **The expansion of the digital perimeter:** With the rise of mobile banking, open APIs, and interconnected systems, the digital ecosystem has become more complex and challenging to protect. Every new access point, from mobile apps to IoT devices, represents a potential entry point for attackers.
- **International regulation and cooperation:** The cross-border nature of bank fraud complicates investigations and the tracking of stolen funds. Furthermore, disparities in data protection and cybersecurity laws between countries make effective coordination to combat these threats more difficult.
- **Reputational risk:** Beyond financial losses, financial institutions face the challenge of maintaining their customers' trust. A security breach can have a lasting impact on an entity's reputation, affecting its relationship with users and its position in the market.

Strategies to mitigate bank fraud

- **Implementation of advanced technologies:** Tools such as artificial intelligence and machine learning enable the identification of anomalous patterns in real time, detecting suspicious transactions before they materialise. Additionally, technologies like blockchain offer solutions for creating more secure and transparent systems.

- **Enhanced authentication:** Multi-factor authentication (MFA) has become a standard for reducing the risk of unauthorised access. Regulations such as PSD2 in Europe have made strong authentication mandatory to protect digital transactions.
- **Ongoing user education**: Investing in cybersecurity awareness programmes is crucial to reduce the effectiveness of social engineering attacks. Customers need to be informed about recognising phishing attempts, maintaining secure passwords, and protecting their devices.
- **Convergence of physical and logical security:** Protecting ATMs, CCTV systems, and internal servers should be integrated with digital strategies. An example of this convergence is the implementation of systems that detect physical tampering in critical devices.
- **Rapid incident response:** The ability to detect and respond to incidents in real time is essential to limit the impact of an attack. This includes establishing Security Operations Centres (SOCs) and adopting Extended Detection and Response (XDR) solutions.
- **International and regulatory collaboration:** Institutions must work jointly with governments and international organisations to share information on emerging threats and strengthen regulations. Initiatives such as cyber intelligence sharing between banks can be key.

Conclusion

Bank fraud is an ever-evolving battle that demands a comprehensive approach. Financial institutions must move beyond reactive solutions and adopt a proactive strategy that combines advanced technology, user education, and cross-sector collaboration. While it is unlikely that fraud will ever be completely eradicated, the goal is to minimise its impact as much as possible, safeguarding not only economic resources but also the trust and security of millions of people worldwide.

Ultimately, cybersecurity should not be seen as an expense but as a strategic investment. Only through a combination of innovation, effective regulation, and a user-centred approach can the challenges of bank fraud in the 21st century be effectively addressed.

Francisco Javier García Lorente
Cybersecurity Project Manager

New year, same attacks

Cyberchronicles by Diego Alonso Fernández and Adrián Álvarez Sánchez

In 2024, cyberattacks saw a significant global increase. During the third quarter, companies worldwide recorded an average of 1,876 attacks per week, marking a 75% rise compared to the same period in 2023 and a 15% increase from the previous quarter. In this cyber chronicle, we reflect on the close of 2024 as a preview of what may lie ahead in 2025.

Unsurprising attacks, unprecedented heights

In 2024, cyberattacks reached historic levels, with global losses exceeding €10 billion. Artificial intelligence (AI) became a double-edged sword, enabling both defence and offence. Attackers leveraged AI to execute highly precise operations, such as banking Trojans and cryptocurrency fraud. Additionally, services like "Phishing-as-a-Service" lowered entry barriers, allowing even inexperienced actors to carry out effective attacks.

The most affected sectors included manufacturing, healthcare, and energy. Attacks targeting critical infrastructure generated global concern, while the rise in ransomware paralysed essential systems. In the United Kingdom, the National Health Service (NHS) suffered an attack that compromised sensitive patient data and disrupted healthcare services.

Europe faced significant impacts from geopolitical tensions. The UK reported a "cyberwar" led by Russia, which utilised AI to attack telecommunications and energy institutions. In France, Anonymous Sudan launched massive attacks in March 2024, disrupting key government services.

In November, zero-day vulnerabilities were discovered in routers and network video recorders (NVRs). These were exploited by the Mirai malware to carry out DDoS attacks, underscoring the urgent need for stronger strategies to protect digital infrastructures.

As the year drew to a close, Spain's National Markets and Competition Commission (CNMC) suffered a cyberattack, resulting in the leak of over 2 billion records related to mobile phone users. This became one of the most severe incidents of the year in Spain.

This year, 2025, has begun with a significant attack on Telefónica, one of the largest telecommunications companies in the world, in which 2.3 GB of confidential data were stolen, raising concerns about corporate security and customer privacy. Although the company responded swiftly, the incident highlighted persistent vulnerabilities even in organisations with advanced infrastructures.

According to subsequent analysis, the attack was facilitated by the use of infostealer malware, which extracted credentials and critical data. This information enabled attackers to deploy social engineering tactics, amplifying the incident's impact. The case illustrates how modern threats combine advanced technological tools with psychological manipulation to maximise their effects.

The attack also underscored the role of AI in automating intrusion and data extraction tactics, allowing attackers to achieve their objectives with speed and precision. The situation reaffirmed the necessity of proactive strategies to address emerging threats.

Meanwhile, NATO has decided to strengthen its presence in the Baltic Sea to protect critical underwater infrastructure following a surge in attacks on submarine cables in recent months. This mission, named "Baltic Sentry," will involve ships, aircraft, and "a small fleet of naval drones," although the Alliance is withholding specific details to avoid aiding potential attackers. The objective is to enhance surveillance capabilities and coordinate efforts to detect threats effectively.

What lies ahead in 2025: the future of cybersecurity

Looking ahead for the rest of the year, experts anticipate an increase in the sophistication of cyberattacks.

AI will enable attackers to launch customised and targeted operations, exploiting specific vulnerabilities from massively collected data. Critical sectors such as healthcare, energy, and transportation infrastructures will continue to be priority targets due to their societal impact.

The proliferation of Internet of Things (IoT) devices opens new doors for attackers, who could use vulnerable networks to carry out mass attacks, such as DDoS.

In response, organisations must invest in early detection technologies, educate their employees on cybersecurity best practices, and collaborate with governments and institutions to share information on emerging threats.

Conclusions

The cybersecurity landscape in 2024 and the start of 2025 have demonstrated that threats evolve rapidly, while defences often lag behind.

Collaboration between the public and private sectors, along with significant investments in advanced technologies and cybersecurity education, will be essential to building a more resilient digital ecosystem.

In a world where technological opportunities and risks go hand in hand, only those who are prepared will thrive. In the face of an uncertain digital future, proactivity and adaptability will be our best defences.

Diego Alonso Fernández
Cybersecurity Analyst

Adrián Álvarez Sánchez
Cybersecurity Architect

Preventive measures against scams

Article by Alejandra Romero Gutiérrez

The detection of fraud, with a preventive approach, is very complex as it is the legitimate user who is carrying out the transaction. In this article, we will review various measures that could enable a higher fraud detection rate, considering the friction with the customer and the financial institution's risk appetite.

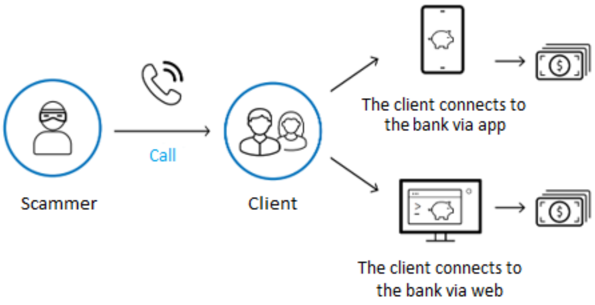
The significant increase in scams, compared to conventional fraud, is causing substantial reputational erosion for financial institutions, concern over the potential assumption of future losses, and significant harm to society in general. This is due to the low cost of scam campaigns for organised fraud teams, alongside substantial economic benefits.

Unlike conventional fraud, where criminals seek to obtain the user's credentials through various methods, in scams, it is the user themselves who performs the deceptive operation. Methods such as device intelligence, geolocation, or artificial intelligence models designed for fraud prevention, among others, on their own, do not yield good results in detecting scams or preventing them from occurring.

Below, we analyse the main attack vectors and solutions that have shown good results.

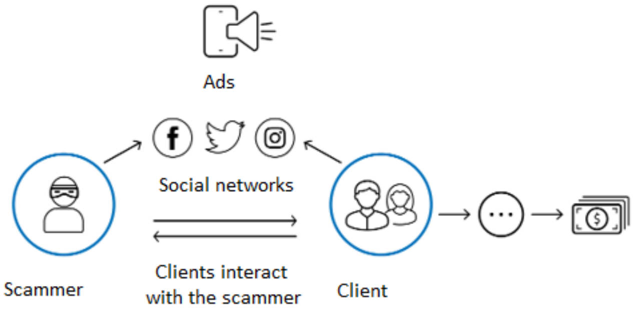
Scam via phone call

The scammer, through a phone call to the victim, creates a stressful situation to pressure them into accessing their bank (via app or website) and transferring a sum of money. This type of attack relies on exploiting the urgency and psychological vulnerability of the user, who, under pressure, acts without proper caution.


Scammer
Call
Client
The client connects to the bank via app
The client connects to the bank via web

Scam via advertisements / social media

The scammer, through advertisements and communications on social media, attracts potential victims and interacts with them until eventually convincing them to transfer their money. This method is very common in investment scams, such as those involving the purchase of goods and rentals. It should also be considered within the attack vectors those scammers who open accounts with financial institutions, either online or in person, to receive the money they have gained from the scams.



Preventive measures

Creation of scoring models

Entities can consider the creation of specific scoring models to improve, for example, the detection of potential fraudsters and money mules or potential scam victims. Based on historical data, various factors can be analysed, such as occupation, products contracted, type of registration, type of communication with the entity (including queries and campaigns), age, transaction history, investments, etc., with the aim of identifying common patterns and subsequently extrapolating them.

These models, in addition to helping prevent fraud, can improve false positives, resolve issues related to account blockages, and contribute to compliance with the identification and reporting of money mule accounts.

Behavioural biometrics

Behavioural patterns, such as mouse or device movements, typing patterns, or session duration, can indicate signs of stress, hesitation, or distraction, which are typical signs when a customer is being guided by a fraudster.

Thus, the use of behavioural biometrics provides an insight into the emotions or intentions of a user during a session and allows real-time identification of social engineering scams. Several market solutions have invested in research and development to model specific behavioural patterns that predict scams.

These tools generally work better when their behavioural biometric signals are orchestrated with transactional profiles using risk engines capable of scoring the risk of potential frauds and triggering real-time intervention actions.

Link analysis

This measure links one or more identification features associated with a suspected fraudulent attack with the identification features of reported money mules or fraudsters.

Several solutions leverage networks of device characteristics linked to individuals labelled with markers indicating fraud association by other consortium members. They have proven effective in detecting potential scams by scoring the risk of outgoing payments based on the links between the account or device characteristics of the beneficiary and the account or device characteristics of reported individuals.

Call in progress

There are solutions that detect when a user is on a phone call and is operating their banking, in order to prevent potential scam situations. Some are capable of detecting whether the call is on WhatsApp.

This functionality should be accompanied by rules to reduce friction with customers and minimise false positives. For example, if the number is on the list of usual beneficiaries.

Interactive interventions with the user

The emerging solution in the market involves increasing friction for customers (typically those in vulnerable groups at risk of being scammed) by altering the transaction completion flow, sending users specific messages about the transaction, and requiring additional factors.

For each type of scam, the most common patterns should be identified so that a real-time message can be sent to the user, requesting a second authentication factor without halting the transaction. This change in the customer journey would help generate doubts in users who may be victims of a potential scam, introduce additional friction for a limited percentage of customers, reduce the need for operational team reviews, and simplify the claims process.

Collaboration

Collaboration between financial institutions in the fight against financial crime, through the sharing of confirmed fraud data, will significantly improve fraud prevention. Moreover, cooperation between financial and non-financial institutions, as well as public entities involved in combating fraud, will provide customers with greater security when carrying out operations.

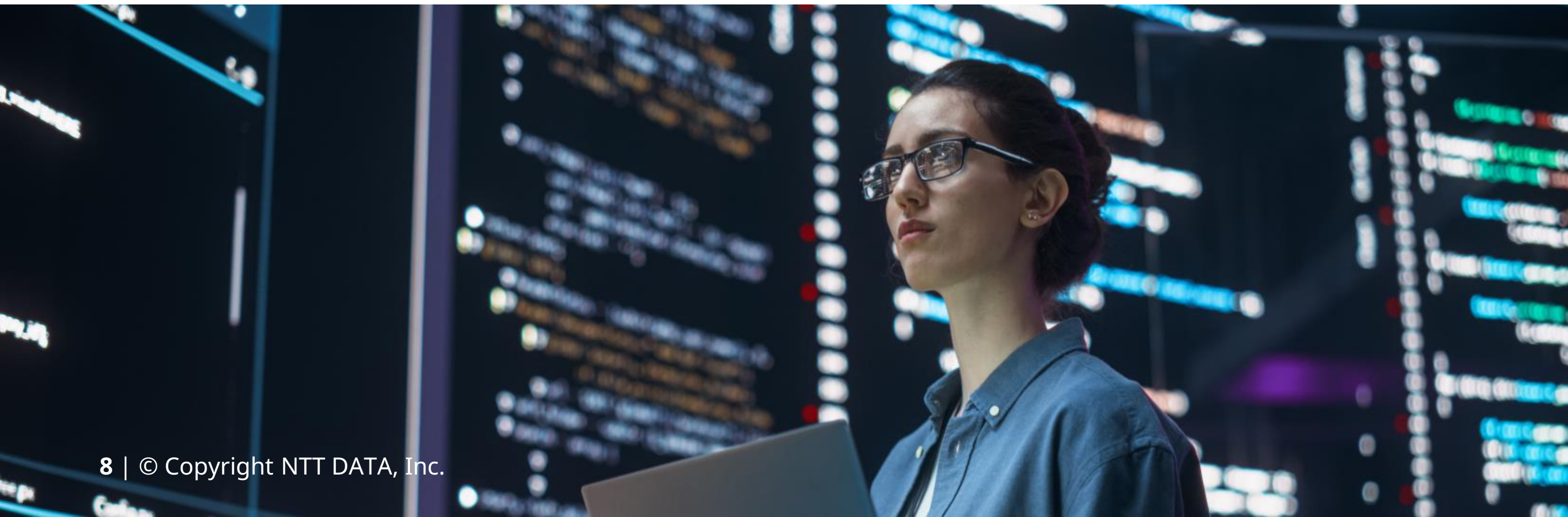
Awareness

Educating and training consumers is essential in the fight against fraud, as the customer is often the weakest link in the security chain.

Understanding the most common methods of fraud and scams enables consumers to recognise warning signs and act before falling victim. Likewise, knowing how to protect oneself reduces the anxiety and stress associated with the possibility of being deceived.

NTT DATA has a highly specialised team in fraud prevention, detection, and management. Our multidisciplinary expertise allows us to advise organisations on strategic decision-making as well as the selection, adaptation, and implementation of tailored technological solutions. With our deep understanding of the entire ecosystem, we offer a 360° perspective and an end-to-end (e2e) approach to ensure maximum effectiveness in fraud mitigation.

Alejandra Romero Gutierrez
FinCrime Director



High cybersecurity standards

Trends by Gerard Marín

The financial sector faces significant cybersecurity challenges in 2025, driven by the use of artificial intelligence and the increased risk surface stemming from increasingly expansive ecosystems. Adding to this is the implementation of the Digital Operational Resilience Act (DORA), aimed at strengthening the sector's ability to manage complex threats. The transition to zero-trust models and advances in quantum-resistant cryptography will be critical to ensuring protection against both current and future risks.

The two major challenges in 2025 will be the use of AI by cybercriminals and the expansion of the risk surface.

Banks and financial institutions are increasingly leveraging artificial intelligence (AI) for threat detection and mitigation. However, cybercriminals have responded by adopting machine learning (ML) techniques to bypass traditional security measures. These attacks are becoming more sophisticated, targeted, and harder to detect, exploiting vulnerabilities with precision. This adversarial use of AI highlights the need for innovative security solutions capable of anticipating and countering evolving threats.

Additionally, in the pursuit of profitability, the financial sector is expanding its reach and forming more relationships with third parties, suppliers, and their providers. This expansion increases the risk surface, as banks may have robust prevention, detection, and response measures against cyberattacks, but their partners may lack similar protections.

This could lead banks, beyond being direct targets of cyberattacks, to becoming victims of cyberattacks aimed at their ecosystem of alliances, suppliers, and other partners.

The implementation of DORA will drive greater investment in cybersecurity

In response to these growing threats, regulatory bodies are introducing stricter frameworks to strengthen resilience across the financial sector. A key milestone in 2025 is the implementation of the Digital Operational Resilience Act (DORA), which came into force on 17 January. This regulation aims to harmonise ICT risk management requirements, ensuring that financial institutions are better prepared to handle systemic risks, including cyber risks.

The financial sector is expected to significantly increase its investments in cybersecurity. Additionally, there is a strong emphasis on implementing robust operational resilience strategies, particularly when adopting emerging technologies, to mitigate the impact of the associated risks.

DORA's comprehensive guidelines will serve as a cornerstone in this regulatory evolution, requiring institutions to adopt proactive risk management measures.

New threats will require zero-trust architectures

Traditional perimeter-based security models are proving inadequate against the complexity of modern cyber threats. By 2025, many organisations are transitioning to a Zero Trust Architecture (ZTA), a model that requires strict identity verification for every user and device attempting to access resources on private networks.

An increase in quantum research is expected to address risks by 2030

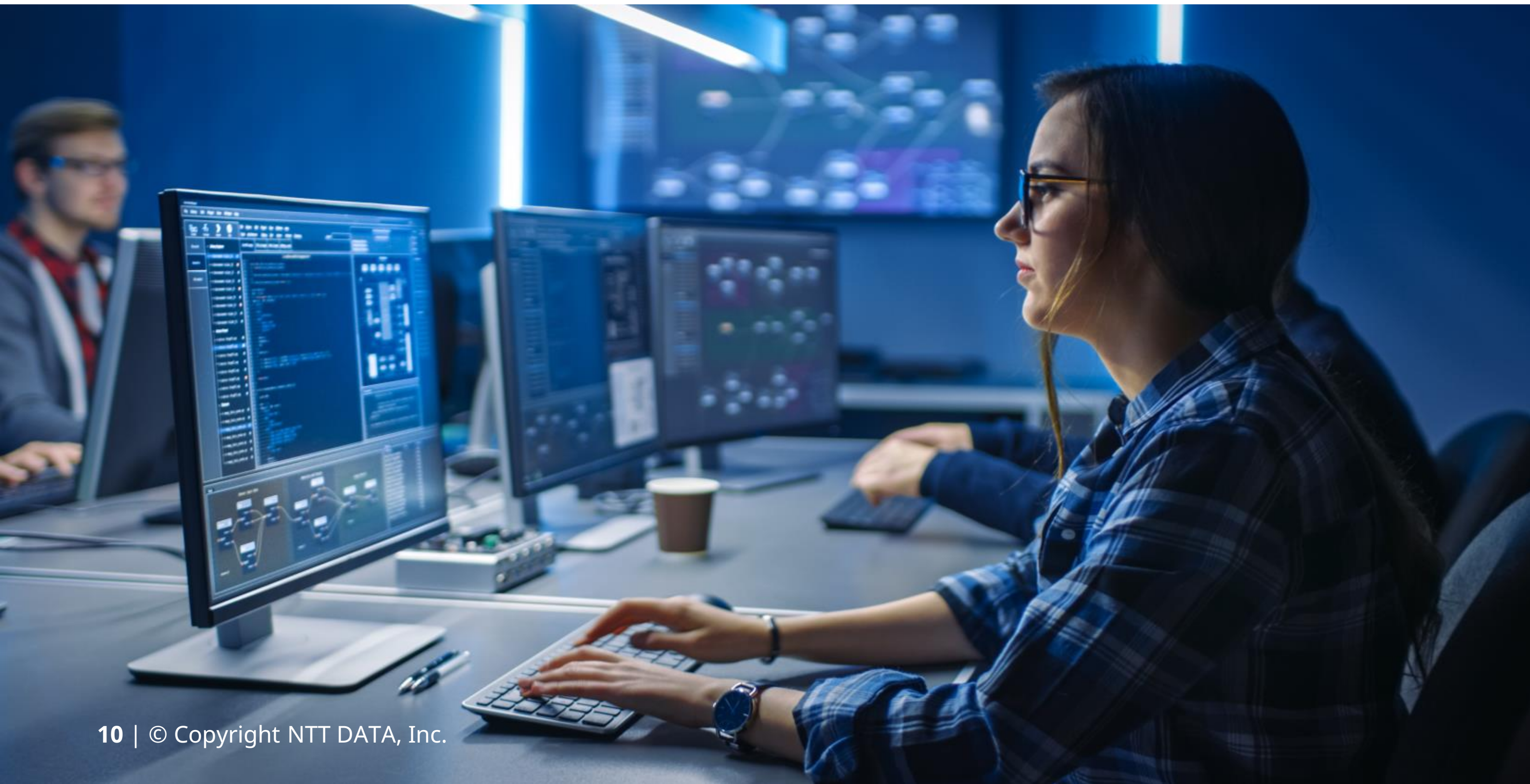
As quantum computing approaches general feasibility, its potential to disrupt current encryption standards looms as a significant threat. Theoretically, quantum computers could break widely used encryption algorithms such as RSA and ECC in a matter of minutes, posing an unprecedented risk to data security.

Although governments have already begun working on this issue, the financial sector should prioritise the development and adoption of quantum-resistant cryptography to counteract this imminent risk. While experts predict that quantum attacks may become practical by 2030, the foundation for resilience must begin now to protect critical infrastructure against future disruptions.

Conclusion

The cybersecurity challenges facing the financial sector in 2025 are formidable, but not insurmountable. Addressing the escalating threat landscape, adapting to regulatory changes like DORA, adopting Zero Trust Architecture, and preparing for quantum risks are essential steps to ensure resilience. By prioritising innovation, collaboration, and proactive risk management, the industry can protect its systems and continue thriving in an increasingly digital world.

Gerard Marín Raventos
Cybersecurity Consultant



Vulnerabilities

Remote code execution vulnerability in Webmin

Date: December 20, 2024
CVE: CVE-2024-12828

CVSS: 9.9

CRITICAL

Description

The Zero Day Initiative team has identified a vulnerability in the Webmin product.

This vulnerability allows an attacker to execute arbitrary code in Webmin. Authentication is required to exploit this vulnerability.

The specific flaw exists in the CGI requests within Webmin. The vulnerability occurs due to the lack of validation of a user-provided string before using it to make a system call. An attacker could exploit this vulnerability to execute code in the context of root.

Solution

Webmin has released an update to fix the vulnerability.

The update is available in a new version on the manufacturer's official GitHub.

Affected products

This vulnerability affects the following Webmin products:

- The manufacturer has stated that Webmin is affected, without specifying any particular version.

References

- incibe.es
- nvd.nist.gov
- zerodayinitiative.com

Vulnerabilities

Critical vulnerability in SonicWall Firewall

Date: January 7, 2025
CVE: CVE-2024-53704 and 3 more

CVSS: 8.2

HIGH

Description

The provider SonicWall has alerted its customers to update their SonicOS firewall devices to address a critical vulnerability.

This vulnerability allows for an authentication bypass that affects SSL VPN connections and SSH service management.

The manufacturer addressed this vulnerability on January 7, 2025, and the provider recommends the immediate installation of this new patch to fix this vulnerability along with other less critical ones.

Solution

This vulnerability has been fixed in the latest security patch from the manufacturer.

To correct this vulnerability, you should update to the following versions:

- Gen 6/6.5 hardware firewalls: SonicOS 6.5.5.1-6n or earlier.
- Gen 6/6.5 NSv firewalls: SonicOS 6.5.4.v-21s-RC2457 or earlier.
- Gen 7 firewalls: SonicOS 7.0.1-5165; 7.1.3-7015 or earlier.
- TZ80 firewalls: SonicOS 8.0.0-8037 or earlier.

Affected products

This vulnerability affects the following versions of the software:

- 6.5.4.15-117 and earlier versions
- 7.1.1-7058 and earlier versions
- Version 7.1.2-7019.

References

- psirt.global.sonicwall.com
- www.incibe.es

Critical SHARP update to mitigate vulnerabilities in routers

Date: December 22, 2024
CVE: CVE-2024-46873 and 2 more

Critical

Description

SHARP has issued an alert regarding multiple critical vulnerabilities affecting certain models of their routers.

If exploited, these vulnerabilities could allow an attacker to execute commands with administrator privileges, gain unauthorised access, and potentially carry out denial-of-service attacks. The most high-risk vulnerabilities are: CVE-2024-45721, CVE-2024-46873, and CVE-2024-54082.

Exploitation of these vulnerabilities could result in attackers stealing sensitive information, disrupting services through denial-of-service attacks, and gaining unauthorised remote control.

Affected products

The products affected by these vulnerabilities are:

- NTT Docomo, Inc: Wi-Fi STATION SH-05L, SH-52B, SH-54C and home 5G HR02
- SoftBank Corp: Pocket Wi-Fi 809SH
- KDDI Corporation: Speed Wi-Fi NEXT W07

Solution

It is recommended to update all affected products to the latest version, depending on the specific product, following the manufacturer's guidelines.

References

- unaaldia.hispasec.com
- nvd.nist.gov
- incibe.es

Security patches for Palo Alto Networks (PAN) products

Date: December 27, 2024
CVE: CVE-2024-3393

High

Description

Palo Alto Networks has released patches to mitigate a critical vulnerability in its device management software.

Specifically, the vulnerability is located in the "DNS Security" section of the software, where it would allow an unauthenticated attacker to exploit firewalls through manually crafted data packets. Executing these instructions would force the device to reboot. Repeating this chain of events would cause the device to enter maintenance mode, leading to a denial of service (DoS).

Due to the severity of the vulnerability, it has been assigned a CVSS score of 8.7, and it is actively being exploited.

Affected products

The security updates affect the following versions:

- PAN-OS 11.2 and earlier
- PAN-OS 11.1 and earlier
- PAN-OS 10.2 and earlier
- PAN-OS 10.1 and earlier

Solution

PAN recommends updating to the following versions:

- PAN-OS 11.2.3
- PAN-OS 11.1.5
- PAN-OS 10.2.10-h12 y 10.2.13-h2
- PAN-OS 10.1.14-h8

References

- gbhackers.com
- security.paloaltonetworks.com
- socradar.io

Events

EspañaSec Cyber Summit

February 11 – 12

The main objective of SpainSec Cyber Summit is to bring together more than 100 cybersecurity leaders from various industries, including banking, automotive, utilities, and manufacturing, fostering collaboration among like-minded professionals.

Over the course of two days, the event will focus on exploring the main trends in cybersecurity strategies, tools, and standards. The agenda will feature educational and interactive sessions designed to promote knowledge generation, strategic planning, and the exchange of experiences among industry experts.

Link

CyberTech Latin America 2025

19 - 20 February

Since its creation in 2017, CyberTech Latin America has served as the bridge connecting the region's leading cybersecurity, business, and innovation ecosystems.

This event, held in collaboration with the Embassy of Israel in Panama, the City of Knowledge, SENACYT, AIG, and other prominent regional partners, offers exclusive access to a high-level meeting. The event brings together government officials, industry leaders, academics, established companies, and dynamic start-ups under one roof.

Link

CIBER2C MX

26 February

The CIBER2C MX Congress is a key cybersecurity event that brings together experts, government representatives, and industry leaders to address threats and solutions in essential sectors such as energy, transportation, and healthcare. Its goal is to safeguard the systems that support the economy and daily life.

Under the motto "Critical Infrastructures in the Crosshairs: The Great Challenge of Cybersecurity," the congress promotes the exchange of strategies and public-private collaboration, fostering a culture of innovation and resilience in the face of the challenges of an interconnected world.

Link

HackOn 2025

February 28 to March 1

HackOn is an event founded in 2019 aimed at cybersecurity professionals and enthusiasts, combining conferences, hands-on workshops, and Capture The Flag (CTF) challenges.

In its upcoming edition, HackOn will explore topics such as artificial intelligence applied to security, ethical hacking, and cyber resilience. With activities for all levels, this event promises to be an educational and collaborative experience that drives technological innovation and professional networking.

Link

Resources

AttackGen

AttackGen is an open-source tool that helps organisations prepare for cyber threats. It uses advanced AI models and the MITRE ATT&CK framework to create incident response scenarios tailored to the organisation's size, sector, and selected threat actors. With features like quick templates for common attacks and an integrated assistant to refine scenarios, AttackGen makes incident planning easy and effective. It is compatible with both enterprise and industrial systems, helping teams stay prepared for real-world threats.

Link

Brainstorm

Brainstorm is a tool that makes web fuzzing more efficient by using local LLMs like Ollama along with ffuf. It analyses the links of a target website and generates intelligent guesses for hidden files, directories, and API endpoints. By learning from each discovery, it reduces the number of requests needed while finding more endpoints compared to traditional wordlists. This tool is perfect for optimising fuzzing tasks, saving time, and avoiding detection.

Link

FuzzyAI

FuzzyAI is a tool that provides organisations with a systematic approach to testing AI models against various adversarial inputs, discovering potential weaknesses in their security systems, and making the development and deployment of AI more secure. At the core of FuzzyAI is a powerful fuzzer capable of exposing vulnerabilities found through more than ten distinct attack techniques, ranging from bypassing ethical filters to uncovering hidden system prompts.

Link

Vulnhuntr

A static Python code analyser that leverages the power of large language models (LLMs) to find and explain complex, multi-step vulnerabilities. Thanks to the capabilities of models like Claude 3.5, the AI has discovered over a dozen remotely exploitable 0-day vulnerabilities targeting open-source projects in the AI ecosystem with more than 10,000 stars on GitHub in just a few hours of operation.

Link

Subscribe to RADAR
up.nttdata.com/suscribetearadar

**Powered by the
cybersecurity
NTT DATA team**

es.nttdata.com