

# CyberSecBrief

Daily Cybersecurity Trends & Insights | 2024-01-01

## Top Stories

### Online retailer PcComponentes says data breach claims are fake **GLOBAL**

BleepingComputer | 2026-01-21 | Emerging Threats & Attack Patterns

PcComponentes, a major technology retailer in Spain, has denied claims of a data breach on its systems impacting 16 million customers, but confirmed it suffered a credential stuffing attack. [...]

### REGULATION | Data Protection Commissioner Confirms Deletion of Kenyans' WorldCoin Biometric Data - BitKE **KENYA**

ODPC Kenya | 2026-01-22 | Regional Focus

REGULATION | Data Protection Commissioner Confirms Deletion of Kenyans' WorldCoin Biometric Data BitKE

### Cisco fixes Unified Communications RCE zero day exploited in attacks **GLOBAL**

BleepingComputer | 2026-01-21 | Emerging Threats & Attack Patterns

Cisco has fixed a critical Unified Communications and Webex Calling remote code execution vulnerability, tracked as CVE-2026-20045, that has been actively exploited as a zero-day in attacks. [...]

### TempoNet: Learning Realistic Communication and Timing Patterns for Network Traffic Simulation **GLOBAL**

arXiv (Security) | 2026-01-23 | Academic Research & Papers

arXiv:2601.15663v1 Announce Type: new Abstract: Realistic network traffic simulation is critical for evaluating intrusion detection systems, stress-testing network protocols, and constructing high-fidelity environments for cybersecurity training. While attack traffic can often be layered into training environments using red-teaming or replay methods, generating authentic benign background traf...

### Multi-Targeted Graph Backdoor Attack **GLOBAL**

arXiv (Security) | 2026-01-23 | Academic Research & Papers

arXiv:2601.15474v1 Announce Type: cross Abstract: Graph neural network (GNN) have demonstrated exceptional performance in solving critical problems across diverse domains yet remain susceptible to backdoor attacks. Existing studies on backdoor attack for graph classification are limited to single target attack using subgraph replacement based mechanism where the attacker implants only one trig...

### What OpenAI's Health Push And Google's AI Rollouts Really Mean For Africa **KENYA**

On 7th January 2026, OpenAI launched the waitlist for the ChatGPT Health model which is expected to provide a specialized model... Source

## Kenya Sharpens Innovation Strategy Through Global Index Alignment **KENYA**

CIO Africa | 2026-01-23 | Regional Focus

As Kenya sharpens its ambition to transition into a first-world economy, innovation is increasingly taking centre stage as both a... Source

## Dception: Real-world Wireless Man-in-the-Middle Attacks Against CCS EV Charging **GLOBAL**

arXiv (Security) | 2026-01-23 | Academic Research & Papers

arXiv:2601.15515v1 Announce Type: new Abstract: The adoption of Electric Vehicles (EVs) is happening at a rapid pace. To ensure fast and safe charging, complex communication is required between the vehicle and the charging station. In the globally used Combined Charging System (CCS), this communication is carried over the HomePlug Green PHY (HPGP) physical layer. However, HPGP is known to suff...

## Side-Channel Attacks on Open vSwitch **GLOBAL**

arXiv (Security) | 2026-01-23 | Academic Research & Papers

arXiv:2601.15632v1 Announce Type: new Abstract: Virtualization is widely adopted in cloud systems to manage resource sharing among users. A virtualized environment usually deploys a virtual switch within the host system to enable virtual machines to communicate with each other and with the physical network. The Open vSwitch (OVS) is one of the most popular software-based virtual switches. It m...

## Connect the Dots: Knowledge Graph-Guided Crawler Attack on Retrieval-Augmented Generation Systems **GLOBAL**

arXiv (Security) | 2026-01-23 | Academic Research & Papers

arXiv:2601.15678v1 Announce Type: new Abstract: Retrieval-augmented generation (RAG) systems integrate document retrieval with large language models and have been widely adopted. However, in privacy-related scenarios, RAG introduces a new privacy risk: adversaries can issue carefully crafted queries to exfiltrate sensitive content from the underlying corpus gradually. Although recent studies h...