Threatsploit Adversary Report

Edition 82

JUNE 2025

Arulselvar Thomas
Founder & Director, Briskinfosec

BriskInfosec™
VULNERABILITY TO VICTORY

www.briskinfosec.com

Monthly Magazine

Introduction :

Dear Readers,

Every month, the Threatsploit Adversary Report delivers a curated overview of the latest global cyberattacks, vulnerabilities, and threat actor activities. We dive deep into real-world incidents that matter most to security teams and decision-makers across industries.

In this edition, we spotlight critical incidents such as the breach at the UnitedHealth Group's Change Healthcare platform, which compromised vast amounts of sensitive data. The FBI's takedown of the LockBit ransomware infrastructure also marks a major disruption in global ransomware operations. Additionally, the exposure of 49 million Dell customer records and the Microsoft Windows Defender SmartScreen vulnerability (CVE-2024-21412) underline the rising stakes in both corporate and consumer digital ecosystems.

This report is built on continuous monitoring, timely threat intelligence, and expert validation. Each edition captures the critical events that shape the threat landscape - from sophisticated breach campaigns to newly disclosed CVEs with high exploitation potential.

Month after month, year after year, our goal remains unchanged: to be your trusted source of clarity in a fast-evolving world of cyber threats. Let this report be your strategic companion in strengthening cyber resilience.

"Awareness isn't built in a day - it's shaped by the breaches, missteps, and wake-up calls we choose not to ignore"

Best regards,

Briskinfosec Threat Intelligence Team.

Contents :

1. New Stealth Malware "Skitnet" Used by Ransomware Gangs to Evade Detection and Maintain Access
2. Malicious Python Packages on PyPI Threaten Open-Source Developers
3. Critical ChatGPT Security Flaw Exploited via Malicious Embedded Images
4. RVTools Website Compromised to Distribute Bumblebee Malware via Infected Installer
5. Trojanized KeePass Installer Distributes Cobalt Strike, Leads to ESXi Ransomware Attack
6. Phishing Campaigns Employ Malicious HTML Files to Spread Horabot Malware
7. Critical Adobe Photoshop Vulnerabilities Allow Arbitrary Code Execution
8. DarkCloud Stealer Campaign Targets Government and Tech Sectors via Obfuscated AutoIt Scripts
9. Katz Stealer Malware Targets Over 78 Chromium and Gecko-Based Browsers
10. Malicious Google Calendar Invites Exploit Invisible Characters to Deliver Malware
11. Samsung Addresses Critical MagicINFO 9 Vulnerability Exploited by Mirai Botnet
12. Google Chrome Zero-Day Flaw CVE-2025-4664 Actively Exploited—Users Urged to Update Immediately
13. Critical Windows DWM Zero-Day Exploited for SYSTEM-Level Privilege Escalation
14. Swan Vector APT Targets Japanese and Taiwanese Institutions with Multi-Stage Malware
15. Critical Windows Remote Desktop Vulnerabilities Allow Remote Code Execution
16. iClicker Website Compromised: Students Targeted with Malware via Fake CAPTCHA
17. ASUS Resolves Critical Remote Code Execution Vulnerabilities in DriverHub Utility
18. PupkinStealer Malware Exploits Telegram Bots to Exfiltrate Sensitive Data
19. Radware Cloud WAF Vulnerabilities Allow Attackers to Bypass Security Filters
20. VMware Tools Flaw Enables Unauthorized File Modifications on Guest VMs
21. Critical Template Injection Vulnerability in Insomnia API Client Leads to Remote Code Execution
22. Chinese APT Group 'UnsolicitedBooker' Deploys MarsSnake Malware in Prolonged Espionage Campaign
23. RedisRaider Campaign Exploits Redis Servers to Deploy Go-Based XMRig Miner
24. Microsoft Issues Emergency Update to Resolve BitLocker Recovery Loop in Windows 10
25. Adidas Korea Data Breach Exposes Customer Information via Third-Party Service Provider
26. Malicious Koishi Plugin Secretly Exfiltrates Chatbot Data via QQ Messaging
27. Hazy Hawk Hijacks Abandoned DNS Records to Distribute Malware via Trusted Domains
28. AWS Default IAM Roles Pose Privilege Escalation Risks Across Services
29. Google Chrome Introduces Automatic Password Change Feature to Enhance User Security
30. Critical Vulnerabilities in Foscam X5 IP Cameras Allow Remote Code Execution

New Stealth Malware "Skitnet" Used by Ransomware Gangs to Evade Detection and Maintain Access

A newly discovered malware named Skitnet is being leveraged by ransomware gangs to infiltrate systems, evade antivirus detection, and maintain persistent remote access. Developed using Rust and Nim, the malware uses stealthy techniques such as DNS tunneling, PowerShell abuse, and remote desktop tools like AnyDesk to operate covertly. Skitnet is capable of taking screenshots, stealing files, and executing commands, often bypassing traditional defenses. It creates persistence through startup folders and registry changes, making it difficult to remove. This malware is particularly dangerous because of its modular design and ability to serve as a precursor to full ransomware deployment.

Attack Type : Command-and-Control

Cause of Issue : Phishing attacks

Industry Type : Managed Service Providers

Malicious Python Packages on PyPI Threaten Open-Source Developers

A recent discovery has unveiled malicious Python packages uploaded to the Python Package Index (PyPI), posing significant risks to open-source developers. These packages are designed to execute harmful code upon installation, potentially compromising developer systems and the software supply chain. The attackers employ obfuscation techniques to evade detection, making it challenging for standard security measures to identify the threat. This incident underscores the vulnerabilities inherent in open-source ecosystems and highlights the need for enhanced scrutiny of third-party packages. Developers are urged to exercise caution and implement stringent security practices when incorporating external libraries into their projects.

Attack Type : Supply Chain Attack

Cause of Issue : Negligence

Industry Type : Software Development Community

Critical ChatGPT Security Flaw Exploited via Malicious Embedded Images

A significant vulnerability (CVE-2025-43714) was identified in ChatGPT, enabling attackers to inject malicious SVG and image files directly into shared chat conversations. This vulnerability facilitates stored Cross-Site Scripting (XSS) attacks, allowing harmful scripts to execute automatically when conversations are reopened or publicly shared. Users exposed to such attacks risk data theft, phishing, or malicious script execution. The security issue stems from ChatGPT's improper handling of SVG files, which inadvertently allows JavaScript execution. OpenAI has temporarily disabled public sharing of conversations as an immediate mitigation measure. A permanent solution to address the underlying issue is currently under development.

Attack Type : Stored Cross-Site Scripting

Cause of Issue : Misconfiguration

Industry Type : Artificial Intelligence

RVTools Website Compromised to Distribute Bumblebee Malware via Infected Installer

The official website for RVTools, a widely-used VMware environment reporting utility, was compromised to serve a trojanized installer embedded with the Bumblebee malware loader. Security researcher Aidan Leon discovered that the malicious installer sideloaded a tampered version.dll file, deploying Bumblebee-a known tool for initiating ransomware attacks and post-exploitation activities. The duration of the compromise and the number of affected users remain unclear. In response, RVTools' official sites, Robware.net and RVTools.com, have been taken offline, and users are advised to verify installer hashes and monitor for suspicious DLL executions. This incident underscores the risks associated with software supply chain attacks.

Attack Type : Supply Chain Attack

Cause of Issue : Supply-Chain

Industry Type : IT Infrastructure

Trojanized KeePass Installer Distributes Cobalt Strike, Leads to ESXi Ransomware Attack

Threat actors have been distributing trojanized versions of the KeePass password manager for at least eight months to install Cobalt Strike beacons, steal credentials, and ultimately, deploy ransomware on the breached network. WithSecure's Threat Intelligence team discovered the campaign after they were brought in to investigate a ransomware attack. The researchers found that the attack started with a malicious KeePass installer promoted through Bing advertisements that promoted fake software sites. As KeePass is open source, the threat actors altered the source code to build a trojanized version, dubbed KeeLoader, that contains all the normal password management functionality. However, it includes modifications that install a Cobalt Strike beacon and export the KeePass password database as cleartext, which is then stolen through the beacon.

Attack Type : Supply Chain Attack

Cause of Issue : Malvertising

Industry Type : IT Infrastructure

Phishing Campaigns Employ Malicious HTML Files to Spread Horabot Malware

Cybersecurity researchers have identified a sophisticated phishing campaign targeting Spanish-speaking users in Latin America, utilizing weaponized HTML files to distribute the Horabot malware. The attack initiates with emails masquerading as legitimate invoices, containing ZIP attachments with malicious HTML files. Upon opening, these files download additional payloads, including HTA files that execute VBScript, AutoIt, and PowerShell scripts. This multi-stage infection chain enables data theft, credential harvesting, and lateral movement within networks. The campaign's stealthy techniques, such as environment checks and fake pop-ups, make detection challenging, emphasizing the need for robust email security measures and user awareness training.

Attack Type : Phishing Attack

Cause of Issue : Phishing

Industry Type : Internet Users

Critical Adobe Photoshop Vulnerabilities Allow Arbitrary Code Execution

Adobe has released critical security updates for Photoshop on both Windows and macOS platforms after discovering multiple severe vulnerabilities that could allow attackers to execute arbitrary code on victims' systems. The security bulletin addresses three critical flaws affecting Photoshop 2025 (version 26.5 and earlier) and Photoshop 2024 (version 25.12.2 and earlier). The most concerning aspect of these flaws is their potential to allow threat actors to execute arbitrary code on affected systems, potentially leading to complete system compromise. Fortunately, Adobe is not aware of any exploits in the wild for any of the issues addressed in these updates.

Attack Type : Arbitrary Code Execution

Cause of Issue : Memory Management Flaws

Industry Type : Creative and Design Professionals

DarkCloud Stealer Campaign Targets Government and Tech Sectors via Obfuscated AutoIt Scripts

In early 2025, Unit 42 researchers identified a sophisticated malware campaign distributing DarkCloud Stealer, an information-stealing malware. The attack initiates with phishing emails containing malicious PDFs that prompt users to download RAR archives from file-sharing services. These archives house AutoIt-compiled executables, which, upon execution, decrypt and run embedded shellcode to deploy the DarkCloud payload. The malware exfiltrates sensitive data, including browser credentials, email passwords, and FTP login information, while employing anti-analysis techniques to evade detection. Notably, the campaign has predominantly targeted government agencies and technology firms across multiple countries, highlighting the need for robust email security and user awareness training.

Attack Type : Phishing

Cause of Issue : Social Engineering

Industry Type : Government Sectors

Katz Stealer Malware Targets Over 78 Chromium and Gecko-Based Browsers

Katz Stealer is a newly identified information-stealing malware posing a significant threat to users of Chromium and Gecko-based browsers. Developed in C and Assembly for lightweight efficiency, it targets credentials, cookies (including version 20+), autofill data, CVV2 codes, OAuth tokens, cryptocurrency wallets, and messaging platforms like Discord and Telegram. The malware's customizable build panel includes anti-virtual machine safeguards and a web-based command-and-control interface for managing stolen data. Its broad targeting of browser architectures and third-party applications, coupled with sophisticated anti-detection mechanisms, underscores the escalating arms race between malware developers and security teams.

Attack Type : Information Stealer Malware

Cause of Issue : Exploitation

Industry Type : Cryptocurrency Holders

Malicious Google Calendar Invites Exploit Invisible Characters to Deliver Malware

Cybercriminals have developed a novel technique to distribute malware by exploiting Google Calendar invites. They embed malicious code within seemingly innocuous characters, specifically using invisible Unicode Private Use Area (PUA) characters disguised as a simple vertical bar ("|"). These characters decode into base64-encoded instructions that connect to attacker-controlled servers via Google Calendar URLs. This method allows the malware to bypass traditional email security measures by leveraging the trust users place in Google services. The attack has been linked to compromised npm packages, including "os-info-checker-es6," which serve as delivery mechanisms for the malicious payloads.

Attack Type : Supply Chain Attack

Cause of Issue : Abuse

Industry Type : Internet Users

Samsung Addresses Critical MagicINFO 9 Vulnerability Exploited by Mirai Botnet

Samsung has released a critical security patch for its MagicINFO 9 Server software, addressing a severe path traversal vulnerability identified as CVE-2025-4632. This flaw, carrying a CVSS score of 9.8, allows unauthenticated attackers to write arbitrary files with system-level privileges, potentially leading to full system compromise. Notably, the vulnerability has been actively exploited in the wild, with threat actors deploying the Mirai botnet shortly after a proof-of-concept was published on April 30, 2025. The issue stems from the improper limitation of pathnames to restricted directories, enabling attackers to bypass previous patches. Samsung urges all users to update to version 21.1052 to mitigate this threat.

Attack Type : Remote Code Execution

Cause of Issue : PathTraversal

Industry Type : Enterprise Display Management Systems

Google Chrome Zero-Day Flaw CVE-2025-4664 Actively Exploited—Users Urged to Update Immediately

Google has released an urgent security update for Chrome to patch a critical vulnerability, CVE-2025-4664, which is being actively exploited in the wild. This high-severity flaw arises from insufficient policy enforcement in Chrome's Loader component, allowing attackers to bypass security policies and potentially execute unauthorized code or perform sandbox escapes. The vulnerability was initially disclosed by security researcher @slonser_ on May 5, 2025. Users are strongly advised to update to Chrome version 136.0.7103.113/.114 for Windows and Mac, and 136.0.7103.113 for Linux, to mitigate this threat.

Attack Type : Cross-Origin Data Leak

Cause of Issue : Bypass

Industry Type : Google Chrome User

Critical Windows DWM Zero-Day Exploited for SYSTEM-Level Privilege Escalation

Microsoft has addressed a critical zero-day vulnerability in the Windows Desktop Window Manager (DWM) Core Library, identified as CVE-2025-30400. This flaw, stemming from a use-after-free memory corruption issue, allows authenticated attackers to escalate privileges to the SYSTEM level. Actively exploited in the wild prior to patching, the vulnerability enables attackers to bypass security boundaries, potentially leading to full system compromise. Microsoft released a fix on May 13, 2025, as part of its Patch Tuesday updates. Users and administrators are strongly advised to apply the latest security updates promptly to mitigate this threat.

Attack Type : Privilege Escalation

Cause of Issue : Use-After-Free

Industry Type : Windows Users

Swan Vector APT Targets Japanese and Taiwanese Institutions with Multi-Stage Malware

A sophisticated cyber-espionage campaign, dubbed "Swan Vector," has been targeting educational and mechanical engineering institutions in Japan and Taiwan. The attack initiates with spear-phishing emails containing ZIP archives that house malicious LNK files disguised as resumes. Upon execution, these files deploy a multi-stage malware chain involving DLL sideloading and advanced evasion techniques. Key components include the Pterois and Isurus implants, which utilize API hashing and direct system calls to evade detection. The final stage involves deploying Cobalt Strike shellcode, with command-and-control communications routed through Google Drive, leveraging OAuth for authentication. Researchers attribute the campaign to East Asian threat actors with medium confidence.

Attack Type : Advanced Persistent Threat

Cause of Issue : Social Engineering

Industry Type : Educational Instutions

Critical Windows Remote Desktop Vulnerabilities Allow Remote Code Execution

Microsoft's May 2025 Patch Tuesday addressed two critical vulnerabilities in Windows Remote Desktop Services : CVE-2025-29966 and CVE-2025-29967. These heap-based buffer overflow flaws in the Remote Desktop Client and Gateway Service, respectively, could allow unauthorized attackers to execute arbitrary code over a network. An attacker controlling a malicious Remote Desktop server could exploit these vulnerabilities when a victim connects using a vulnerable client, leading to potential system compromise. While no active exploitation has been reported, Microsoft has rated these vulnerabilities as "Critical," emphasizing the importance of applying the latest security updates promptly.

Attack Type : Remote Code Execution

Cause of Issue : Overflow

Industry Type : Windows Users

iClicker Website Compromised: Students Targeted with Malware via Fake CAPTCHA

The iClicker website, a widely used student engagement platform, was compromised between April 12 and April 16, 2025, in a sophisticated ClickFix attack. Attackers injected a fake CAPTCHA prompt instructing users to verify their humanity. Upon interaction, a malicious PowerShell script was silently copied to the user's clipboard. Users were then guided to execute this script via the Windows Run dialog, leading to the installation of malware. The payload varied based on the target, with some users receiving benign files to avoid detection, while others were infected with malware granting attackers full device access. This incident underscores the evolving tactics of social engineering attacks.

Attack Type : Social Engineering Attack

Cause of Issue : Defacement

Industry Type : Educational Institutions

ASUS Resolves Critical Remote Code Execution Vulnerabilities in DriverHub Utility

ASUS has addressed two critical security vulnerabilities in its DriverHub utility, identified as CVE-2025-3462 and CVE-2025-3463, which could allow attackers to execute arbitrary code remotely. The first flaw involves an origin validation error, while the second pertains to improper certificate validation. Exploitation could occur through crafted HTTP requests and malicious .ini files, enabling attackers to run unauthorized code via the AsusSetup.exe binary. Security researcher MrBruh reported these issues, leading to patches released on May 9, 2025. Users are strongly advised to update their DriverHub installations to the latest version to mitigate potential risks.

Attack Type : Remote Code Execution

Cause of Issue : Validation Bypass

Industry Type : ASUS DriverHub Users

PupkinStealer Malware Exploits Telegram Bots to Exfiltrate Sensitive Data

PupkinStealer is a lightweight yet potent .NET-based information-stealing malware that emerged in April 2025. Targeting Windows users, it focuses on extracting sensitive data such as browser credentials from Chromium-based browsers, session information from Telegram and Discord, desktop files (e.g., .pdf, .txt, .jpg), and screenshots. The malware compresses the harvested data into a ZIP archive, embedding system metadata, and exfiltrates it via the Telegram Bot API to attacker-controlled bots. Notably, PupkinStealer lacks advanced anti-analysis or persistence mechanisms, relying on its simplicity and the abuse of legitimate platforms like Telegram to evade detection and facilitate data theft.

Attack Type : Information Stealer Malware

Cause of Issue : Telegram Bot API

Industry Type : Internet Users

Radware Cloud WAF Vulnerabilities Allow Attackers to Bypass Security Filters

Security researchers have identified two critical vulnerabilities in Radware's Cloud Web Application Firewall (WAF), designated as CVE-2024-56523 and CVE-2024-56524. These flaws enable attackers to bypass the WAF's security filters, potentially exposing underlying web applications to malicious inputs. CVE-2024-56523 involves sending specially crafted HTTP GET requests with random data in the request body, which the WAF fails to properly filter. CVE-2024-56524 exploits insufficient validation of user-supplied input containing special characters, allowing various payloads to bypass security controls. Organizations relying on Radware's Cloud WAF are advised to ensure they are running the latest version and implement additional security measures.

Attack Type : Web Application Firewall Bypass

Cause of Issue : Improper Input Validation

Industry Type : Cloud based Industry

VMware Tools Flaw Enables Unauthorized File Modifications on Guest VMs

VMware has addressed a moderate-severity vulnerability (CVE-2025-22247) in VMware Tools that permits non-administrative users to manipulate files within guest virtual machines. This insecure file handling flaw allows attackers with limited privileges to perform unauthorized file operations, potentially leading to privilege escalation or malicious activities within the VM environment. The vulnerability affects VMware Tools versions 11.x.x and 12.x.x on Windows and Linux platforms, with macOS remaining unaffected. VMware has released version 12.5.2 to mitigate this issue and urges organizations, especially those with multi-user VM environments, to apply the updates promptly to prevent potential exploitation.

Attack Type : Privilege Escalation

Cause of Issue : File Manipulation

Industry Type : IT Organizations

Critical Template Injection Vulnerability in Insomnia API Client Leads to Remote Code Execution

A critical vulnerability, identified as CVE-2025-1087, has been discovered in Kong's Insomnia API client, affecting versions prior to 11.0.2. This flaw arises from insufficient validation of user-supplied input when processing template strings, allowing attackers to inject malicious templates that are evaluated within the application's JavaScript context. Exploitation of this vulnerability can lead to arbitrary code execution on the user's machine, potentially compromising sensitive environment variables and system integrity. Given Insomnia's widespread use among developers and DevOps teams for interacting with various API endpoints, users are strongly advised to update to version 11.0.2 or later to mitigate this risk.

Attack Type : Remote Code Execution

Cause of Issue : Insufficient Input Validation

Industry Type : Software Development

Chinese APT Group 'UnsolicitedBooker' Deploys MarsSnake Malware in Prolonged Espionage Campaign

A China-aligned threat actor, dubbed "UnsolicitedBooker," has been conducting a multi-year cyber-espionage campaign targeting a Saudi Arabian organization. The attackers employed spear-phishing emails, masquerading as flight ticket confirmations from Saudia Airlines, to deliver a malicious Microsoft Word document. This document contained a VBA macro that, when executed, deployed a previously undocumented backdoor named "MarsSnake." MarsSnake establishes communication with a remote server, enabling unauthorized access and data exfiltration. The campaign, observed in 2023, 2024, and 2025, underscores the persistent efforts of state-sponsored actors to infiltrate and monitor strategic targets in the Middle East.

Attack Type : Advanced Persistent Threat

Cause of Issue : Social Engineering

Industry Type : Governmental Sectors

RedisRaider Campaign Exploits Redis Servers to Deploy Go-Based XMRig Miner

A newly identified cryptojacking campaign, dubbed "RedisRaider," targets publicly accessible Redis servers to deploy a Go-based malware that installs the XMRig cryptocurrency miner on Linux hosts. The attackers scan the IPv4 space to locate vulnerable Redis instances and use legitimate configuration commands to inject malicious cron jobs. These cron jobs execute Base64-encoded shell scripts that download and run the RedisRaider binary, which serves as a dropper for the XMRig miner. The campaign also employs anti-forensic techniques, such as short key time-to-live settings and database configuration changes, to evade detection and hinder analysis.

Attack Type : Cryptojacking

Cause of Issue : Misconfigured Redis Servers

Industry Type : Linux-Based Redis Servers

Microsoft Issues Emergency Update to Resolve BitLocker Recovery Loop in Windows 10

On May 19, 2025, Microsoft released an emergency out-of-band update (KB5061768) to address a critical issue causing Windows 10 systems to boot into BitLocker recovery screens following the installation of the May 2025 security updates. The problem stemmed from the KB5058379 update, which led to unexpected termination of the Local Security Authority Subsystem Service (LSASS), triggering automatic repair processes and persistent boot loops.

The issue primarily affected enterprise systems running Windows 10 version 22H2, Enterprise LTSC 2021, and IoT Enterprise LTSC 2021 with Intel vPro processors and Trusted Execution Technology (TXT) enabled.

Microsoft advises affected organizations to install the KB5061768 update promptly and, if necessary, temporarily disable Intel VT for Direct I/O (VTD/VTX) and TXT in BIOS/UEFI settings to facilitate the update process.

Attack Type : System Disruption via Faulty Update

Cause of Issue : Faulty Security Update

Industry Type : IT Industries

Adidas Korea Data Breach Exposes Customer Information via Third-Party Service Provider

Adidas Korea has confirmed a data breach resulting from unauthorized access through a third-party customer service provider. The incident affected customers who contacted Adidas's customer service centers in 2024 or earlier. Compromised data includes names, email addresses, phone numbers, and, in some cases, birthdates and physical addresses. Financial information such as passwords and payment details were not impacted. Adidas has notified affected customers, reported the breach to relevant Korean authorities, and is collaborating with information security specialists to investigate the incident and implement enhanced security measures to prevent future occurrences.

Attack Type : Data Breach

Cause of Issue : Vendor Compromise

Industry Type : Retail and Fashion Industry

Malicious Koishi Plugin Secretly Exfiltrates Chatbot Data via QQ Messaging

A malicious npm package named koishi-plugin-pinhaofa has been discovered within the Koishi chatbot framework, which is widely used for developing cross-platform bots on platforms like QQ, Telegram, and Discord. This plugin covertly monitors all messages processed by the chatbot, specifically targeting those containing eight-character hexadecimal strings-often indicative of sensitive data such as API tokens or authentication codes.

Upon detection, the plugin exfiltrates the entire message content to a hardcoded QQ account, leveraging the bot's own messaging capabilities to avoid detection. The simplicity of the JavaScript code used and its integration into the trusted environment of the chatbot make this supply chain attack particularly insidious.

Attack Type : Supply Chain Attack

Cause of Issue : Malicious Plugin Installation

Industry Type : Banking Sector

Hazy Hawk Hijacks Abandoned DNS Records to Distribute Malware via Trusted Domains

A threat actor known as Hazy Hawk has been exploiting misconfigured DNS records, specifically abandoned CNAME entries pointing to decommissioned cloud services, to hijack subdomains of prominent organizations. By registering these unused cloud resources, the attackers gain control over the associated subdomains, which are then used to host malicious content, scams, and adware.

This tactic leverages the credibility of reputable domains to enhance the visibility and trustworthiness of malicious sites in search engine results, facilitating the distribution of harmful content while evading detection. Affected entities include government agencies, universities, and major corporations.

Attack Type : DNS Hijacking

Cause of Issue : Misconfiguration DNS

Industry Type : Government Sector

AWS Default IAM Roles Pose Privilege Escalation Risks Across Services

Cybersecurity researchers have identified that default Identity and Access Management (IAM) roles in Amazon Web Services (AWS), automatically created by services such as SageMaker, Glue, EMR, and Lightsail, often possess overly permissive policies like AmazonS3FullAccess. These broad permissions can be exploited by attackers to escalate privileges, traverse laterally across services, and potentially compromise entire AWS accounts. A notable example includes the open-source Ray framework, which generates a default IAM role with extensive S3 access. AWS has responded by modifying the AmazonS3FullAccess policy for these default roles to mitigate the associated risks.

Attack Type : Privilege Escalation

Cause of Issue : Overpermissioning

Industry Type : AWS Services

Google Chrome Introduces Automatic Password Change Feature to Enhance User Security

Google has unveiled a new feature in its Chrome browser that empowers the built-in Password Manager to automatically update compromised passwords. When Chrome detects that a user's credentials have been compromised during sign-in, it prompts the user with an option to fix the issue automatically. On supported websites, Chrome can generate a strong replacement password and update it for the user without manual intervention. This enhancement aims to reduce friction in maintaining account security, allowing users to safeguard their accounts more efficiently by streamlining the password update process.

Attack Type : Credential Compromise

Cause of Issue : Compromised Passwords

Industry Type : Internet Users

Critical Vulnerabilities in Foscam X5 IP Cameras Allow Remote Code Execution

Security researchers have uncovered multiple critical vulnerabilities in Foscam X5 IP cameras, specifically in firmware version 2.40 and earlier. These flaws reside in the UDTMediaServer component, which exposes unauthenticated endpoints susceptible to buffer overflow attacks. Exploiting these vulnerabilities enables attackers to execute arbitrary code with root privileges, potentially opening a Telnet service on port 4321 and granting full device control. Additionally, the RtspServer component is vulnerable to CVE-2018-4013, a known stack-based buffer overflow in the LIVE555 RTSP server library. Despite multiple disclosure attempts, Foscam has not addressed these issues, leaving users at risk.

Attack Type : Remote Code Execution

Cause of Issue : Unpatched Buffer Overflow

Industry Type : Surveillance Systems organization

Top Critical CVEs – May 2025

1. CVE-2025-20188

A vulnerability in the Out-of-Band AP Image Download feature of Cisco IOS XE for Wireless LAN Controllers allows unauthenticated remote attackers to upload arbitrary files due to a hard-coded JWT. By sending crafted HTTPS requests, attackers can exploit this flaw to perform path traversal and execute commands with root privileges.

ATTACK TYPE | *Directory Traversal*

2. CVE-2025-46828

An unauthenticated SQL Injection vulnerability exists in WeGIA up to version 3.3.0, in the /html/socio/sistema/get_socios.php endpoint's query parameter. Attackers can exploit it to execute arbitrary SQL, potentially leading to data theft, auth bypass, or full database compromise. The issue is fixed in version 3.3.1.

ATTACK TYPE | *Sql Injection*

3. CVE-2025-26389

A vulnerability in OZW672 and OZW772 (all versions below V8.0) allows unauthenticated remote attackers to execute arbitrary code with root privileges via unsanitized input parameters in the exportDiagramPage endpoint of the web service.

ATTACK TYPE | *Code Execution*

4. CVE-2025-23123

A heap buffer overflow vulnerability in UniFi Protect Cameras (version 4.75.43 and earlier) allows a malicious actor with management network access to execute remote code (RCE) on affected devices.

ATTACK TYPE | *Code Execution*

5. CVE-2025-29972

An SSRF vulnerability in Azure enables an authorized attacker to spoof network requests across the internal network.

ATTACK TYPE | *SSRF*

Top Critical CVEs – May 2025

6. CVE-2025-35003

Apache NuttX RTOS Bluetooth Stack (HCI/UART) has buffer overflow and memory bounds flaws allowing crashes, DoS, or code execution via crafted packets. Affected: 7.25 to <12.9.0. Fixed in 12.9.0.

ATTACK TYPE | *Denial of Service*

7. CVE-2025-3605

Frontend Login and Registration Blocks plugin (≤1.0.7) allows unauthenticated attackers to change any user's email via improper validation, enabling account takeover.

ATTACK TYPE | *Privilege Escalation*

8. CVE-2025-48340

A Cross-Site Request Forgery (CSRF) vulnerability in Danny Vink User Profile Meta Manager (up to version 1.02) enables privilege escalation.

ATTACK TYPE | *CSRF*

9. CVE-2025-47548

A Server-Side Request Forgery (SSRF) vulnerability exists in Varun Dubey Wbcom Designs - Activity Link Preview For BuddyPress (up to version 1.4.4), allowing attackers to perform SSRF attacks.

ATTACK TYPE | *SSRF*

10. CVE-2024-6159

The Push Notification for Post and BuddyPress WordPress plugin (before version 1.9.4) allows unauthenticated users to exploit a SQL injection vulnerability due to improper sanitization and escaping of a parameter in an AJAX action.

ATTACK TYPE | *Sql Injection*

"Every Second Counts
defend smarter defend stronger"

+91 44 4352 4537 | +91 73059 79769
contact@briskinfosec.com | www.briskinfosec.com