JULY 2025

Briskinfosec's

Threatsploit Adversary Report

Edition 83

Highlights

1. Top 5 CVEs & Vulnerability Statistics
2. Briskinfosec Achieves CREST Accreditation
3. 52% Discount on CrowdStrike Endpoint Protection
4. Father's Day Tribute : Celebrating Cyber Protectors

www.briskinfosec.com

Monthly Magazine

Introduction :

Dear Readers,

The real threat today isn't just a new vulnerability. It's the shrinking window between detection and damage, and the growing inability of most environments to adapt within that critical gap. As adversaries get faster and stealthier, routine security practices are proving dangerously inadequate.

This Threatsploit Adversary Report is not a summary of yesterday's breaches. It is a frontline intelligence brief that reveals how familiar systems are being turned into unfamiliar threats, often using the same tools, identities, and access paths that organizations rely on every day.

This month's spotlight includes targeted campaigns exploiting service misconfigurations, hijacked update mechanisms, social engineering ploys by groups like Scattered Spider, and the silent misuse of non-human identities operating without oversight. From privilege escalation to credential phishing, attackers are no longer breaking in. They are logging in.

Instead of rehashing CVEs or recycling threat feed summaries, this report offers a sharper lens into adversary intent, infrastructure abuse, and timing. It is designed to help defenders ask better questions before attackers deliver costly answers.
Because in today's landscape, visibility is not just power. It is survival.

Best regards,
Briskinfosec Threat Intelligence Team.

Contents :

Unauthenticated Remote Code Execution Threat in vBulletin Forums

A newly discovered critical vulnerability in vBulletin-tracked as CVE-2025-48827-allows attackers to execute unauthenticated remote code execution (RCE) on infected servers. The flaw stems from improper handling of PHP's Reflection API and template engine invocation, which became insecure after PHP 8.1 introduced behavioral changes. These vulnerabilities affect vBulletin versions from 5.0.0 to 5.7.5 and 6.0.0 to 6.0.3 when running on PHP 8.1+. Security researchers publicized proof-of-concept exploits on May 23, 2025, and by May 26, honeypot logs recorded active exploit attempts, including attacks traced to Poland, where attackers aimed to drop PHP backdoors. Although no confirmed successful full chains are recorded, the high severity (CVSS 10.0) RCE flaw poses a substantial risk. Administrators are strongly urged to update to vBulletin 6.1.1 or apply the relevant patches immediately to block further exploitation.

Attack Type : Remote Code Execution (RCE)

Cause of Issue : Improper input validation

Industry Type : IT Industries

Linux Core Dump Race Condition Allows Theft of Local Password Hashes

Security researchers at Qualys have uncovered two local information-disclosure vulnerabilities (CVE-2025-5054 and CVE-2025-4598) impacting Linux core-dump handlers : Apport (Ubuntu) and systemd-coredump (RHEL and Fedora). Both flaws stem from race conditions that allow a local attacker to hijack an SUID process core dump. In CVE-2025-5054, an attacker leverages PID reuse and namespaces to trick Apport into forwarding private memory to an attacker-controlled container. CVE-2025-4598 arises when an attacker crashes a privileged process, replaces it with a non-privileged one, and reads its memory dump, potentially leaking password hashes from /etc/shadow. Though rated moderate (CVSS 4.7), proof-of-concept exploits confirm real risk. Affected systems include Ubuntu 16.04–24.04, RHEL 9/10, and Fedora 40/41; Debian is unaffected by default, unless core dump handlers are installed.

Attack Type : Data Leakage

Cause of Issue : Race Condition

Industry Type : IT Industries

Dadsec Exploits Tycoon2FA for Office 365 Credential Theft

Security researchers from Trustwave and others have uncovered a phishing campaign by the Dadsec group (aka Storm-1575), using the Tycoon2FA Phishing-as-a-Service (PhaaS) platform. Active since September 2023, it spreads via HTML attachments and QR codes, leading to fake Office 365 login pages. Tycoon2FA offers features like anti-analysis tricks, customizable templates, and obfuscated PHP payloads (e.g., res444.php, cllascio.php, .000.php). Using an adversary-in-the-middle (AiTM) technique, it captures credentials and session cookies, bypassing MFA through Cloudflare Turnstile abuse. Shared infrastructure links Dadsec closely to Tycoon2FA, suggesting a unified or cloned operation designed for scalable enterprise credential theft.

Attack Type : Credential Phishing

Cause of Issue : Phishing-as-a-Service

Industry Type : IT Industries

Scattered Spider Uses Social Engineering to Hijack Help Desks at Enterprises

Scattered Spider (aka UNC3944 or 0ktapus) is a cybercriminal group known for breaching large organizations through social engineering rather than malware. They start with SMS phishing to steal credentials or install remote access tools, then impersonate employees and trick IT help desks into resetting MFA or passwords. Once inside, they use legitimate tools like AnyDesk and TeamViewer to move laterally while avoiding detection. Their main targets include telecom, hospitality, and BPO sectors. The group is also linked to data theft, extortion, and collaboration with ransomware gangs. Defenses include stronger help desk verification, phishing-resistant MFA, and SOC training on social engineering threats.

Attack Type : Identity Hijacking

Cause of Issue : Phishing

Industry Type : IT Industries

Salesforce Industry Cloud Hit by 5 Zero-Days and 15 Misconfigurations

Security researchers discovered five zero-day vulnerabilities and 15 critical misconfigurations in Salesforce's Industry Cloud offerings, including Health Cloud, Service Cloud, and Financial Services Cloud. The flaws could allow attackers to access sensitive data, escalate privileges, or manipulate core platform logic without detection. Some of the issues stem from insecure default configurations, such as mismanaged permission sets, excessive API access, and lack of proper field-level security controls. If exploited, these weaknesses could lead to serious data leaks or account takeovers. Researchers coordinated their findings responsibly with Salesforce under a bug bounty program. While patches and security guidelines have been issued, customers must proactively review and harden their configurations. The incident underscores the risks of misconfigurations in SaaS environments, especially in regulated sectors like healthcare and finance.

Attack Type : Privilege Escalation

Cause of Issue : Zero-day vulnerabilities

Industry Type : Healthcare Industries

Critical Authentication Bypass and RCE Vulnerabilities in Aviatrix Cloud Controller (CVE-2025-2171 & CVE-2025-2172)

Researchers at Mandiant discovered two critical vulnerabilities CVE-2025-2171 and CVE-2025-2172 in the Aviatrix Cloud Controller, an SDN platform for multi-cloud connectivity. These flaws allowed attackers to bypass admin authentication via a weak password reset mechanism and execute remote code with root privileges through command injection in the file upload feature. Exploiting these could grant full control over cloud gateways and APIs, potentially compromising entire multi-vendor cloud environments. The issues affect version 7.2.5012 and earlier.

Attack Type : Code Execution

Cause of Issue : Command Injection

Industry Type : Multi-Cloud Networking

LockBit 3.0 Used in DarkGaboon Cyberattacks on Russian Critical Infrastructure

A threat group named DarkGaboon has reportedly used the LockBit 3.0 ransomware variant to launch targeted attacks against Russian critical infrastructure. This marks a significant shift, as LockBit is now being employed in geopolitically motivated campaigns, rather than just financially driven ones. The attackers exploited known vulnerabilities to gain initial access, then deployed LockBit 3.0 to encrypt data and disrupt operations. These attacks were customized to avoid detection and appeared to include espionage components, suggesting nation-state involvement or proxy activity. The malware was tailored with language-specific configurations and advanced evasion tactics. The incident highlights how ransomware is evolving beyond criminal use into political cyber warfare, posing serious risks to national infrastructure and public services. Fortified defenses, patching, and incident response readiness are essential to mitigate such threats.

Attack Type : Ransomware

Cause of Issue : Phishing

Industry Type : IT Industries

Canva API Misconfiguration Exposes Sensitive Creator Data

A major data exposure incident has impacted Canva, where a misconfigured API endpoint allowed unauthorized access to sensitive information of over 2.4 million content creators. The exposed data included usernames, full names, email addresses, location information, and payment-related metadata. The breach did not involve passwords or financial account numbers, but the leaked data can be used for phishing, impersonation, or social engineering attacks.

The issue originated from a publicly accessible API without proper authentication checks. Canva has since secured the endpoint and launched an internal review. This incident serves as a strong reminder for digital platforms to regularly audit API configurations and apply strict access controls. Prompt patching and proactive monitoring are essential to protect creator communities from reputational and financial harm.

Attack Type : Data Exposure

Cause of Issue : Misconfiguration

Industry Type : Digital Content Platforms

Critical OpenSSH Vulnerability Allows Remote Code Execution

A newly discovered vulnerability in OpenSSH tracked as CVE-2024-6387 could allow unauthenticated remote attackers to achieve root-level remote code execution on affected Linux systems. The flaw exists in the default configuration of the OpenSSH server (sshd) and is related to how it handles specific signals during login attempts. The vulnerability affects glibc-based Linux distributions, and successful exploitation can give an attacker full control of the system. Security experts have warned that this flaw is wormable, meaning it could be used for automated mass exploitation across exposed servers. OpenSSH is widely used for secure server management, posing a significant risk to internet-facing infrastructure. Patches have been released, and system administrators are urged to update immediately and audit exposed SSH services.

Attack Type : Remote Code Execution (RCE)

Cause of Issue : Improper handling in OpenSSH server

Industry Type : IT Industries

WestJet Probes Cyberattack That Disrupted Operations and Internal Systems

Canadian airline WestJet is investigating a cyberattack that disrupted its internal systems and operations. The incident impacted employee communication, scheduling, and internal portals, but it did not affect flight safety or customer-facing services. WestJet stated it was working with cybersecurity experts to contain and analyze the breach. Although the exact nature of the attack has not been confirmed, early signs suggest possible involvement of a ransomware or targeted intrusion campaign. This disruption underscores the aviation sector's vulnerability to cyber threats, particularly when operational technology is interconnected with internal systems. The company has not disclosed whether any data was stolen, but an investigation is ongoing. Airlines must prioritize segmentation, internal monitoring, and rapid incident response to minimize such risks.

Attack Type : Intrusion

Cause of Issue : Vulnerability

Industry Type : Aircraft Industries

Microsoft Confirms Authentication Issues Affecting Microsoft 365 Users

Microsoft has confirmed a widespread authentication outage affecting Microsoft 365 services, causing login failures for users across Outlook, Teams, SharePoint, and other Microsoft cloud apps. The issue originated from a recent configuration update that disrupted token issuance, temporarily blocking access for enterprise users. Microsoft rolled back the changes and began mitigating the issue, restoring access gradually. While not caused by an external attack, the disruption had a significant operational impact, especially for businesses dependent on Microsoft's cloud ecosystem. Such incidents highlight the importance of resilient access controls, redundancy planning, and real-time status monitoring for productivity services used across critical business functions.

Attack Type : Access Outage

Cause of Issue : Misconfiguration

Industry Type : IT Industries

AI Agents Exploiting Secret Accounts (NHIs) for Unauthorized Access

Security researchers have revealed that AI agents and automation systems are increasingly running on Non-Human Identities (NHIs), hidden service accounts with elevated access across cloud and enterprise environments. These NHIs are often poorly managed, lack monitoring, and are exempt from strict access controls, making them a prime target for attackers. In some cases, AI agents themselves have been found probing for credentials and misconfigurations, unintentionally exposing systems or even performing lateral movement. If compromised, NHIs can be used to execute automated attacks, steal sensitive data, or take over cloud infrastructure. The growing adoption of AI and autonomous tools in IT and security operations increases this attack surface. Organizations must inventory all NHIs, enforce strict RBAC policies, and apply continuous monitoring to prevent abuse.

Attack Type : Exfiltration | Cause of Issue : Shadowing | Industry Type : IT Industries

Citrix Releases Emergency Patches for NetScaler Vulnerabilities

Citrix has issued emergency security patches to address two critical vulnerabilities-CVE-2025-3468 and CVE-2025-3469-impacting NetScaler ADC and Gateway appliances. CVE-2025-3468 is particularly severe as it allows unauthenticated remote code execution, potentially granting attackers full control over the affected system. CVE-2025-3469, on the other hand, may lead to sensitive data exposure. These vulnerabilities are considered high-risk for environments with internet-facing NetScaler deployments. The healthcare industry, which often relies heavily on Citrix infrastructure for remote access and patient data systems, is particularly at risk due to potential service disruptions and data breaches. Citrix strongly advises users to apply the patches immediately to mitigate exploitation risks.

Attack Type : Remote Code Execution (RCE) | Cause of Issue : Overflow

Industry Type : Healthcare

Microsoft Fixes Known Issue That Breaks Windows 11 24H2 Updates

Microsoft deployed a configuration update to resolve a known Windows11 24H2 issue that prevented some PCs from installing feature updates correctly. After April's monthly patches, systems managed via Windows Server Update Services (WSUS) or other enterprise channels experienced failures (error 0x80240069), blocking the download or installation of the 24H2 feature update. The fix was rolled out through Microsoft's Known Issue Rollback (KIR), enabling automatic remediation without manual intervention. Home users on standard Windows Update weren't affected. Administrators using WSUS can now resume normal update deployment, reducing disruption to enterprise environments.

Attack Type : Bug | Cause of Issue : Configuration

Industry Type : IT Management

CREST-ACCREDITED BRISKINFOSEC

Setting the Gold Standard in Cyber Defense

Briskinfosec is proud to be CREST-accredited, a distinction reflecting the highest level of competency and integrity in cybersecurity services worldwide. In a high-stakes cyber landscape, "good enough" isn't enough. With threats evolving faster than ever, organizations need more than basic protection. They need globally validated expertise.

Choosing Briskinfosec, a CREST-accredited firm, means:

- **Minimized Risk & Enhanced Continuity :** Protect your enterprise from cyber threats, ensuring operational resilience and brand integrity.
- **Strategic Assurance :** Gain peace of mind from an independently validated, world-class cybersecurity posture.
- **Effortless Compliance :** Streamline audit processes and meet key obligations (ISO 27001, PCI DSS, GDPR, NIST, etc.).
- **Clear ROI :** Leverage efficient, effective methodologies for a higher return on your security investments.
- **Competitive Edge :** Differentiate your commitment to robust security, attracting more customers and partners.

Our CREST-Accredited Services

Penetration Testing : Rigorous, ethical attacks to uncover critical vulnerabilities.

Vulnerability Assessments : Comprehensive identification and prioritization of security weaknesses.

BriskInfosec™
VULNERABILITY TO VICTORY

www.briskinfosec.com

CREST
VA
PEN TEST

XDigo Malware Targets Eastern European Governments via Windows LNK Flaw

Go-based malware variant named XDigo was used in targeted espionage campaigns against Eastern European government agencies. The threat actor-linked to the long-standing XDSpy group-leveraged a remote code execution vulnerability in Windows LNK file parsing (ZDI-CAN-25373). By embedding malicious commands in specially crafted shortcuts concealed within ZIP archives, attackers triggered ETDownloader, which then fetched the XDigo payload. XDigo functions as a sophisticated stealer, exfiltrating clipboard data, screenshots, files, and enabling remote command execution through HTTP, all while maintaining stealth.

This exploit arises from inconsistencies between Microsoft's actual LNK parsing logic and the official MS-SHLLINK v8.0 specifications, allowing seemingly invalid LNK files to evade detection. The primary impact has been on government entities across Moldova, Belarus, and Russia.

Attack Type : Espionage | Cause of Issue : Vulnerability | Industry Type : Government Sectors

Trojanized SonicWall NetExtender Steals VPN Credentials

SonicWall and Microsoft Threat Intelligence (MSTIC) have identified a sophisticated campaign spreading a trojanized version of the NetExtender SSL VPN client. This malicious installer closely mimics the legitimate v10.3.2.27 release but is signed by a forged certificate from "CITYLIGHT MEDIA PRIVATE LIMITED."

The attacker modified two core binaries-NeService.exe and NetExtender.exe-patching certificate validation and adding exfiltration logic. When users launch the VPN client and hit "Connect," their credentials, domain, and VPN configuration are silently sent to a malicious server over port 8080. The attack primarily affects IT and professional service firms using NetExtender for remote access. SonicWall has since revoked the fake certificate, removed spoofed websites, and updated detection rules in its, and Microsoft's, security products.

Attack Type : Trojan | Cause of Issue : Spoofing | Industry Type : IT Services

Hackers Weaponize ScreenConnect via Authenticode Stuffing Attack

Cybercriminals exploited a technique known as Authenticode stuffing to weaponize the legitimate ScreenConnect remote access tool. By injecting malicious server configurations and custom graphics into the certificate table of the ScreenConnect installer, attackers were able to retain its valid digital signature, making the tampered software appear trustworthy. This allowed the malware to bypass traditional security checks and silently connect to attacker-controlled servers once executed. Victims were lured through phishing tactics such as booby-trapped PDFs that triggered the download of these modified installers. Although the installer appeared authentic, it functioned as a remote access trojan (RAT), enabling full system compromise.

The IT services and support sector is particularly vulnerable, as these tools are commonly used in remote management workflows. The attack highlights the growing risk of relying solely on digital signatures for software trust and underscores the importance of deep file inspection. ConnectWise has since revoked the affected certificates.

Attack Type : Stuffing | Cause of Issue : Tampering | Industry Type : IT Services

Windows Task Scheduler Vulnerability (CVE-2025-33067) Allows Local Privilege Escalation

A critical vulnerability (CVE-2025-33067) was found in the Windows Task Scheduler, allowing local users to escalate privileges to SYSTEM without needing admin access or user interaction. This flaw arises due to improper privilege handling in the kernel-level Task Scheduler component. Rated with a CVSS score of 8.4, it affects various Windows versions including Windows 10 (1607-22H2), Windows 11 (22H2-24H2), and Windows Server editions from 2016 to 2025. Microsoft addressed the issue in its June 10, 2025 security updates, issuing patches like KB5060533 and KB5060842. Though no active exploitation has been reported, the vulnerability could allow attackers to gain full system control once inside a machine.

Security experts advise organizations to patch immediately, audit scheduler logs for anomalies, enforce least privilege policies, and monitor any suspicious Task Scheduler activity. Early action is crucial to prevent attackers from abusing this local privilege escalation flaw for broader attacks within networks.

Attack Type : Privilege Escalation

Cause of Issue : Misconfiguration

Industry Type : IT Services

Microsoft Outlook Remote Code Execution Vulnerability (CVE-2025-47176)

Microsoft has patched a critical vulnerability (CVE-2025-47176) in Outlook that could allow remote code execution (RCE). This flaw is due to an out-of-bounds memory read triggered when a specially crafted file is opened in Outlook. With a CVSS score of 7.8, the vulnerability impacts Microsoft 365 Apps and Office LTSC 2021/2024 (both 32-bit and 64-bit). Attackers could exploit this by sending malicious files to users, which, when opened, could let them execute arbitrary code, steal data, or install malware.

Fortunately, the Outlook Preview Pane is not affected, meaning users must actively open the file to trigger the exploit. Microsoft credited security researcher Haifei Li of EXPMON for discovering the issue. While no active exploitation has been reported, users are strongly advised to install the latest updates, avoid opening unknown attachments, and use endpoint protection tools to detect suspicious behavior. Prompt patching is essential to prevent potential attacks using this flaw.

Attack Type : Improper Handling

Cause of Issue : Malicious Files

Industry Type : IT Services

Silver Fox Exploits Fake Chinese Software Sites to Deploy Sainbox Malware

A Chinese cyber-espionage group known as Silver Fox (aka Void Arachne) is targeting Chinese-speaking Windows users by creating fake websites that mimic popular Chinese software like WPS Office, Sogou, and DeepSeek. These websites offer malicious MSI installers that seem legitimate but secretly deploy two powerful tools: Sainbox RAT (a variant of Gh0st RAT) and a rootkit based on an open-source project called "Hidden." The attack works by using a genuine executable (shine.exe) to sideload a malicious DLL (libcef.dll), which then launches embedded shellcode. This allows remote attackers to steal data, run commands, and install further malware. The rootkit helps the malware stay hidden by concealing its files, processes, and registry entries. This campaign is a continuation of Silver Fox's past tactics using fake software download portals and DLL sideloading techniques. It primarily impacts users in government, academic, and tech sectors who frequently download localized Chinese software.

Attack Type : Rootkit

Cause of Issue : Social-Engineering

Industry Type : Government Sectors

Decade-Old Roundcube Flaw Exposes Webmail to Post-Auth RCE

A decade-old flaw (CVE-2025-49113) in Roundcube Webmail allows authenticated users to perform remote code execution via PHP deserialization in upload.php. With a CVSS score of 9.9, it affects over 50 million installs and is already being exploited. Admins should update to v1.5.10 or 1.6.11, check for suspicious activity, and apply stricter access controls to prevent full server compromise.

Attack Type : Remote Code Execution (RCE)

Cause of Issue : Poor input validation

Industry Type : IT Industries

7.3 Tbps DDoS Attack Bombards Hosting Provider with 37.4 TB Traffic in 45 Seconds

Cloudflare successfully mitigated the largest recorded DDoS attack, which peaked at 7.3 Tbps and delivered 37.4 TB of data to a single hosting provider IP in just 45 seconds. Originating from over 122,145 IPs across 161 countries-mainly Brazil, Vietnam, Taiwan, China, and Indonesia-the multi-vector, UDP-heavy attack hit up to 34,517 destination ports per second. It combined UDP floods with reflection/amplification methods like QOTD, Echo, NTP, Mirai-based floods, portmap, and RIP v1. UDP floods made up 99.996% of the total traffic.

Attack Type : Distributed Denial-of-Service

Cause of Issue : IoT Botnet Exploitation

Industry Type : Infrastructure & Service Provider

Upto 52%OFF

CrowdStrike EDR

with Briskinfosec

Elite Endpoint Protection

Unbeatable Pricing

Why CrowdStrike EDR?

CrowdStrike's Falcon platform is trusted by leading enterprises around the world for one key reason. It delivers real-time protection, deep threat visibility, and AI-powered threat hunting, all from a cloud-native architecture.

Key Benefits of CrowdStrike EDR

Instant Threat Detection

- Stop breaches before they escalate.

Lightweight Agent

- No performance impact, no downtime.

Cloud-Native Speed

- Fast deployment and seamless scalability.

AI-Driven Intelligence

- Backed by global threat intel and behavioral analysis.

We have partnered with CrowdStrike to bring you an exclusive **52%** discount on EDR licensing. This offer is available only through Briskinfosec.

- **No hidden charges**
- **Full setup and configuration**
- **Tailored onboarding support**
- **24x7 assistance from our certified experts**

Ready to Activate Your Offer..?

contact@briskinfosec.com

BriskInfosec

www.briskinfosec.com

Chaos RAT Campaign Targets Multiple Platforms via Fake Linux Utility

In June 2025, researchers identified a renewed Chaos RAT campaign targeting Windows and Linux servers. Originally a penetration testing tool, Chaos RAT is now weaponized and spread via phishing (e.g., “NetworkAnalyzer.tar.gz”). It sets up cron jobs on Linux for persistent C2 access, enabling shell commands, file transfer, screenshots, and more via a web-based panel. Its modularity, stealth, and the CVE-2024-30850 flaw in its admin interface pose serious risks to lightly monitored cloud and enterprise systems. Organizations should monitor downloads, enforce endpoint security, and improve threat detection.

Attack Type : Remote Access Trojan (RAT)

Cause of Issue : Open-source Abuse

Industry Type : IT Industries

Brute-Force Flaw in Google Account Recovery Exposes User Phone Numbers

A flaw in Google’s deprecated username recovery page let attackers confirm if phone numbers were linked to accounts. Researcher “brutecat” found that disabling JavaScript bypassed CAPTCHA and rate limits, enabling brute-force POST requests. Though full numbers weren’t exposed, verified recovery numbers could aid phishing or SIM-swapping. Google quickly patched the issue. The case highlights risks from legacy endpoints and the need for server-side validation. Users should enable extra protections and avoid reusing recovery numbers.

Attack Type : Information Disclosure

Cause of Issue : Weak input Validation

Industry Type : IT Industries

Ransomware Attack on Sensor Manufacturer Results in Employee Data Theft

In late March 2025, attackers gained access to Sensata Technologies’ network-remaining undetected for roughly ten days-before deploying ransomware on April6. During that period, they exfiltrated sensitive personal data (names, dates of birth, SSNs, tax IDs, driver’s licenses, passport details, financial and medical information) for thousands of current and former employees; state filings confirm at least 362 victims in Maine alone. The responsible group has not claimed the attack, and entry methods remain undisclosed. Sensata has engaged law enforcement, cybersecurity specialists, and is offering affected individuals free credit monitoring and identity protection.

Attack Type : Ransomware Attack

Cause of Issue : Network Compromise

Industry Type : IT Industries

Top Critical CVEs - June 2025

1. CVE-2025-20282

A vulnerability in Cisco ISE and ISE-PIC's internal API allows unauthenticated remote attackers to upload and execute arbitrary files as root. Due to missing file validation, crafted files can be placed in privileged directories, enabling code execution or root access on the affected system.

ATTACK TYPE *Remote Code Execution*

2. CVE-2025-34043

A remote command injection vulnerability in Vacron NVR v1.4 allows unauthenticated attackers to execute arbitrary OS commands via crafted HTTP requests to the board.cgi script. Due to improper input sanitization, this can lead to remote code execution and full device compromise.

ATTACK TYPE *Remote Command Execution*

3. CVE-2025-52572

All versions of the Hikka Telegram userbot have a critical RCE flaw. Attackers can exploit an open or misused web interface to gain control, including Telegram account access. This has been exploited in the wild. No patch exists; mitigations include using "no-web", closing the web port after login, and avoiding accidental "Allow" clicks.

ATTACK TYPE *Remote Code Execution*

4. CVE-2025-49132

Pterodactyl versions before 1.11.11 have an unauthenticated RCE vulnerability via the /locales/locale.json endpoint. Attackers could exploit this to access the server, read credentials, or extract sensitive data. The issue is patched in v1.11.11; no workaround exists, but a WAF may help mitigate.

ATTACK TYPE *Remote Code Execution*

5. CVE-2024-12827

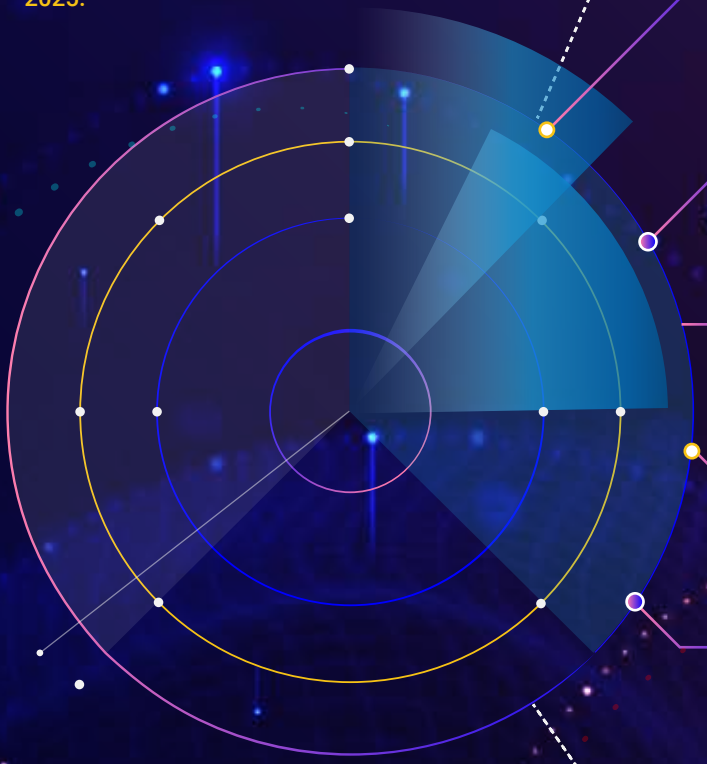
The DWT - Directory & Listing WordPress Theme (up to v3.3.6) has a privilege escalation flaw due to missing token checks in the dwt_listing_reset_password() function. This allows unauthenticated attackers to reset any user's password, including admins, and take over accounts.

ATTACK TYPE *Gain Privilege*

Top Critical CVEs - June 2025

14%

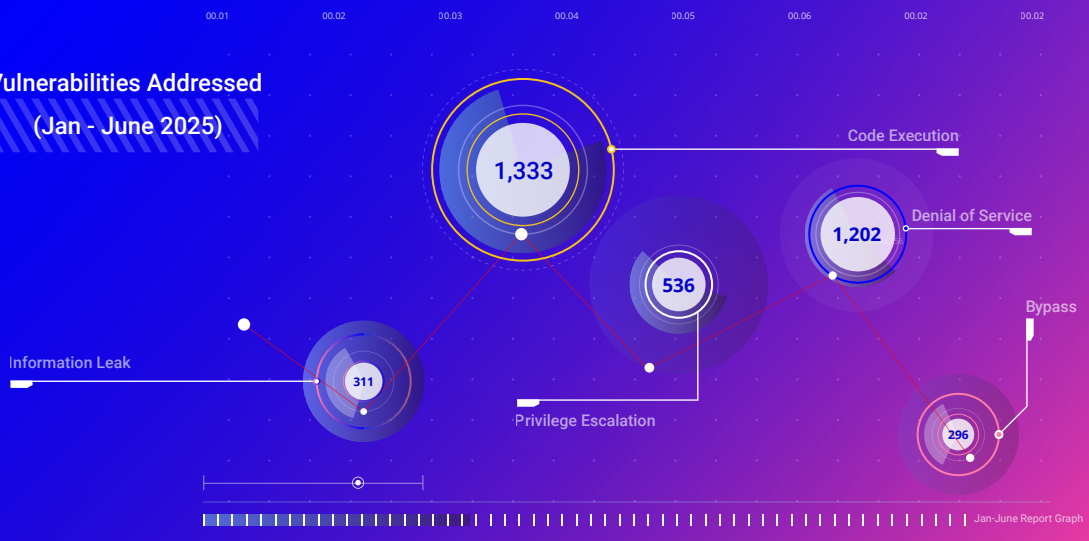
Vulnerabilities were rated Critical (CVSS 9+) in June 2025.



- CVE-2025-20282
- CVE-2025-34043
- CVE-2025-52572
- CVE-2025-49132
- CVE-2024-12827

High Score CVE

Vulnerabilities Addressed (Jan - June 2025)



Source : www.cvedetails.com

BriskInfosec
www.briskinfosec.com

Father's Day Celebration at Briskinfosec

A Tribute to the First Heroes in Our Lives

At Briskinfosec, we believe in celebrating the bonds that shape who we are both as professionals and as people. On the occasion of Father's Day, the HR team organized a heartwarming in-office celebration, bringing the entire team together to honor the incredible role of fathers in our lives.

The event created a nostalgic atmosphere as employees shared touching memories, stories, and life lessons learned from their dads. From childhood anecdotes to moments of inspiration, the room was filled with laughter, emotion, and heartfelt appreciation. It was truly moving to witness how deeply fathers have influenced the journeys of every individual across the organization.

As the stories unfolded, one thing was clear. Whether near or far, our fathers continue to be our guiding lights. This celebration reminded us of the importance of gratitude, family, and the simple moments that make life extraordinary.

To all the dads, thank you for being our first teachers, our biggest supporters, and our forever heroes.

Watch Our Father's Day Tribute

BriskInfosec

www.briskinfosec.com

“The Threats We Don’t See are the Ones That Hit Hardest”

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