THREATSPLOIT

ADVERSARY REPORT

95th Edition | July 2026

www.briskinfosec.com

Dear Reader

Defending an enterprise today means securing a perimeter without physical boundaries. As organizations rely on interconnected cloud ecosystems, adversaries are shifting away from brute-forcing gateways to exploit trusted relationships within your digital supply chain.

This month, we track a dangerous convergence targeting developer pipelines and SaaS ecosystems. Threat actors are poison-dropping dependencies, hijacking unmaintained code repositories, and weaponizing stolen OAuth tokens to bypass authentication. By manipulating the very infrastructure your teams trust to build and run your business, attackers turn software updates and cloud integrations into direct lines of infiltration.

At the same time, the war on the network edge is intensifying. We observe an influx of zero-day exploits engineered to blind endpoint defenses and turn security gateways against internal networks. When malware can terminate security agents at the kernel level and leak raw memory from enterprise proxies, traditional alerting frameworks fall silent.

This report strips away the noise to deliver granular visibility into these operational risks. Reorganized into five strategic threat vectors, each entry breaks down the technical mechanics of a modern exploit paired with an immediate defensive action. Use this data as your roadmap to cutting off lateral movement and reclaiming systemic integrity.

- Briskinfosec Threat Intelligence Team

Supply Chain and Developer Pipeline Security

1. Malicious JetBrains IDE Plugins Caught Siphoning Developer API Keys

A newly discovered campaign highlights a rising threat vector targeting developers through trusted software marketplaces. At least 15 malicious plugins posing as legitimate AI coding assistants were discovered on the JetBrains Marketplace. These trojanized add-ons covertly monitor developer environments. The moment a user inputs an API access key for platforms like OpenAI, SiliconFlow, or DeepSeek, the plugin intercepts the credential and exfiltrates it in plaintext to an attacker-controlled server.

Attack Type : Malicious IDE Plugins / Credential Theft

Root Cause : Trojanized AI Coding Assistants

The Bottom Line : Implement strict marketplace blocklists and continuously audit active developer environment extensions.

2. Atomic Arch Campaign Weaponizes Linux Packages with Stealth eBPF Rootkits

Threat actors have targeted the Arch Linux User Repository (AUR) in a highly coordinated supply chain assault. By hijacking over 400 orphaned or unmaintained AUR software packages, the attackers successfully injected malicious scripts into the installation pipelines of unsuspecting users. The compromise deploys an info-stealer alongside a sophisticated eBPF-based rootkit. Because eBPF runs directly inside the Linux kernel space, the rootkit can easily bypass traditional endpoint monitoring tools to maintain persistent access.

Attack Type : Software Supply Chain / Infostealer

Root Cause : Hijacked Orphaned AUR Packages

The Bottom Line : Monitor eBPF program loading and restrict package installations to vetted upstream repositories.

3. Sapphire Sleet Backdoors Mastra AI npm Packages via Typosquatting

The North Korean state-sponsored threat group Sapphire Sleet has execution workflows in their crosshairs. The attackers published over 140 malicious npm packages targeting developers working with the Mastra AI ecosystem. By utilizing a typosquatted version of a common utility tool, the threat actors tricked developers into importing malicious dependencies into their codebases. Once integrated, the backdoored packages allow the actors to compromise developer systems and position themselves for downstream enterprise supply chain breaches.

Attack Type : Typosquat Supply Chain Attack

Root Cause : Hijacked Dormant Maintainer Accounts

The Bottom Line : Enforce dependency pinning and mandate automated software bill of materials validation.

4. Rogue npm Packages Mimic PostCSS Tools to Deploy Windows Remote Access Trojans

A set of malicious open-source packages designed to compromise software development infrastructure has been identified on the npm registry. The packages pose as legitimate PostCSS CSS processing utilities but contain hidden install scripts. When a developer or automated CI/CD pipeline fetches these dependencies, the hidden scripts execute silently, downloading and installing a fully functional Windows Remote Access Trojan (RAT) to seize control of the underlying host.

Attack Type : Developer Pipeline Compromise

Root Cause : Typosquatted Malicious npm Packages

The Bottom Line : Restrict pipeline execution permissions and utilize registry proxies to block unvetted packages.

Third Party and SaaS Ecosystem Risk

5. Salesforce Halts Klue App Following Icarus OAuth Token Theft

Salesforce took immediate action to disable the third-party Klue Battlecards application following a significant integration breach dubbed Icarus. Cybercriminals successfully compromised the SaaS application's underlying ecosystem and targeted the active OAuth tokens used to sync data between Klue and enterprise Salesforce instances. By stealing these trusted tokens, the attackers bypassed traditional authentication barriers to directly access and exfiltrate sensitive CRM data and enterprise customer accounts.

Attack Type : Third-Party Integration Breach

Root Cause : Stolen OAuth Tokens via SaaS App

The Bottom Line : Audit third-party OAuth permissions regularly and strictly enforce least-privilege SaaS access.

6. Nintendo Employee Records Exposed via Compromised TinyPulse Survey Platform

An external vendor breach has resulted in the exposure of internal employee data at gaming giant Nintendo. Threat actors successfully breached TinyPulse, a third-party SaaS platform utilized by organizations to run anonymous employee feedback surveys and engagement metrics. After compromising the cloud service provider, the attackers accessed and exfiltrated sensitive HR and employee information, utilizing the stolen data to launch subsequent extortion campaigns against the primary organization.

Attack Type : Third-Party SaaS Data Theft / Extortion

Root Cause : Third-Party Survey Compromise

The Bottom Line : Treat employee-facing SaaS vendors as critical infrastructure and mandate formal vendor risk audits.

7. External Licensing Vendor Breach Exposes Millions of Texas Agency Records

The Texas Parks and Wildlife Department suffered a massive data exposure stemming entirely from a compromise at an external technology partner. Threat actors successfully breached the networks of a third-party SaaS vendor responsible for managing state licensing systems. The unauthorized access allowed the attackers to exfiltrate a database containing the personal records of approximately 3 million citizens, demonstrating how vendor vulnerabilities directly compromise government agency data.

Attack Type : Third-Party Vendor Data Breach

Root Cause : Compromised SaaS License Vendor

The Bottom Line : Encrypt citizen data at rest and require vendors to verify independent security controls.

Advanced Malware and Ransomware Operations

8. Gentlemen Ransomware Gang Equips Affiliates with GentleKiller EDR Bypass Suite

The Gentlemen ransomware-as-a-service (RaaS) operation is actively distributing a specialized defense evasion toolkit to its affiliates. This suite is designed to systematically blind security teams by disabling endpoint detection and response (EDR) agents before the final ransomware payload drops. The core tool, GentleKiller, features eight distinct variants that masquerade as legitimate software. It weaponizes the Bring Your Own Vulnerable Driver (BYOVD) technique, abusing trusted kernel drivers to terminate over 400 security processes across 48 major enterprise defense products, including CrowdStrike, SentinelOne, Microsoft Defender, and ESET.

Attack Type : EDR Killer / Defense Evasion

Root Cause : Vulnerable Driver (BYOVD) Abuse

The Bottom Line : Lock down driver loading policies and enforce strict application whitelisting to block unauthorized kernel drivers.

9. High Capability Rokarolla Android Trojan Targets Banking and Crypto Apps

A sophisticated mobile threat named Rokarolla has surfaced, focusing on credential theft and financial fraud across the mobile ecosystem. This advanced Android banking trojan features a massive arsenal of 137 remote execution commands and targets 217 distinct banking and cryptocurrency apps. The malware is distributed via malicious websites masquerading as official TikTok or Chrome updates. Once installed, it tricks users into enabling Android Accessibility services, allowing the malware to log screen PINs, read SMS codes, and deploy fake HTML overlays to steal credentials in real-time.

Attack Type : Android Banking Trojan

Root Cause : Overlay and Accessibility Abuse

The Bottom Line : Block unvetted application sideloading and restrict Android Accessibility permissions via mobile device management.

You Can't Fix the Risks You Can't **Measure**

Every organization has cybersecurity gaps.
The question is: **Do you know yours?**

Over the past six months, our 7-Layer Cybersecurity Assessment has helped organizations uncover critical security gaps across key cybersecurity domains. The findings below highlight the most common risks identified during assessments conducted between January and June 2026.

Insights from 500+ bSAFE Assessments

- **72%** — **Vulnerability Management Gaps**
  Critical vulnerabilities remain unpatched, increasing the risk of exploitation.
- **68%** — **Identity & Access Gaps**
  Weak identity controls, excessive privileges, or missing MPA expose organizations to unauthorized access.
- **61%** — **AI Governance Gaps**
  Organizations are adopting AI rapidly without adequate governance and security controls.
- **57%** — **Third-Party Risk Gaps**
  Vendor and supply chain security assessments are often incomplete or outdated.
- **54%** — **Cloud Security Gaps**
  Cloud misconfigurations and weak security controls continue to put sensitive data at risk.
- **48%** — **Incident Response Gaps**
  Many organizations lack a tested incident response plan to effectively detect, contain, and recover from cyber incidents.

How Does Your Organization Compare?

Measure your cybersecurity maturity with **bSAFE Score.**

Check Now

BriskInfosec™
VULNERABILITY TO VICTORY

10. ScarCruft Leverages Spoofed Microsoft Alerts to Deploy Stealthy NarwhalRAT

The North Korean state-sponsored threat group ScarCruft (APT37) is conducting targeted spear-phishing campaigns aimed at defense and government targets. The attackers send highly convincing emails mimicking automated Microsoft Account security notifications. These emails contain a malicious ZIP attachment containing an LNK file. Once clicked, it executes a complex, multi-stage, fileless infection chain that loads a new malware strain called NarwhalRAT directly into memory. The RAT captures keystrokes, logs audio, and uses commercial cloud APIs as dead-drop command control points.

Attack Type : Spear-Phishing / RAT

Root Cause : Impersonation of Microsoft Alerts

The Bottom Line : Implement advanced email authentication protocols and monitor for unexpected administrative scripts executing from LNK files.

11. ClickFix Campaigns Use Compromised WordPress Sites to Drop Triple Threat Loaders

The operators behind the widespread ClickFix social engineering campaigns have adjusted their delivery infrastructure to expand their reach. Attackers are now injecting malicious scripts into compromised WordPress websites to present users with fraudulent browser updates or CAPTCHA verification checks. If a user follows the fake prompts, they are tricked into pasting attacker-supplied PowerShell code directly into their terminal. This immediately downloads and launches the BabaDeda, Lorem Ipsum, or Potemkin malware loaders, which go on to deploy infostealers across the corporate network.

Attack Type : ClickFix Social Engineering / Loaders

Root Cause : Fake Update and Verification Lures

The Bottom Line : Conduct user awareness training focusing on terminal copy-paste tricks and block outbound script execution.

12. Operation Endgame Takes Down SocGholish Infrastructure and Seizes Servers

A coordinated international law enforcement initiative named Operation Endgame has delivered a severe blow to global cybercrime networks. The operation successfully disrupted the core infrastructure of the notorious SocGholish malware-delivery network. Law enforcement authorities seized 106 command and control servers and successfully cleaned approximately 15,000 compromised websites that were actively hosting fake browser update templates designed to infect corporate networks with ransomware.

Attack Type : Malware-Loader Takedown

Root Cause : Fake Browser Update Delivery

The Bottom Line : Keep web browsers centrally updated and leverage web filtering to block known malicious redirection domains.

13. Malicious WhatsApp VBScript Campaign Abuses ManageEngine RMM Tools

An ongoing phishing campaign is utilizing WhatsApp as an initial entry vector into corporate networks. Attackers distribute malicious VBScript files disguised as standard office documents via chat attachments. When a user opens the attachment, the script silently executes and abuses legitimate, dual-use ManageEngine Remote Monitoring and Management (RMM) tools. By leveraging trusted, signed administration utilities, the attackers can establish persistent remote access and control over endpoints without triggering traditional antivirus software.

Attack Type : Phishing / RMM Abuse

Root Cause : Malicious VBScript via WhatsApp

The Bottom Line : Restrict the execution of unsigned VBScripts and strictly log all active RMM software execution.

14. New OXLOADER Campaign Weaponizes Google Ads to Push CastleStealer Malware

A sophisticated malvertising pipeline has been identified using paid Google Ads to manipulate search engine results for popular software utilities. Unsuspecting users seeking legitimate applications are directed to cloned, malicious landing pages that serve the OXLOADER payload. This delivery mechanism utilizes advanced DLL side-loading techniques to bypass local endpoint security tools. Once executed, the loader establishes a foothold and drops CastleStealer, an aggressive information-stealing utility designed to harvest system credentials and session tokens.

Attack Type : Malvertising / Infostealer Loader

Root Cause : Google Ads DLL Side-Loading

The Bottom Line : Deploy enterprise ad-blocking extensions and implement strict application control policies to block unexpected DLL loading.

Critical Infrastructure and Edge Device Exploitation

15. Cisco Patches Actively Exploited Catalyst SD WAN Manager Directory Traversal Flaw

Cisco has released urgent patches to address a zero-day vulnerability, tracked as CVE-2026-20262, impacting its Catalyst SD-WAN Manager software. The security flaw stems from insufficient input and path validation inside the web management console. Remote, unauthenticated threat actors are actively exploiting this path traversal vulnerability in the wild, allowing them to perform arbitrary file writes on the underlying operating system and ultimately gain full, unauthorized administrative control over core enterprise software-defined networks.

Attack Type : Path Traversal / Arbitrary File Write

Root Cause : Insufficient File-Path Validation

The Bottom Line : Apply the emergency Cisco SD-WAN patches immediately and restrict access to management interfaces.

16. CISA Warns of Active Root Exploitation in LiteSpeed cPanel Plugin

The Cybersecurity and Infrastructure Security Agency (CISA) has added a critical vulnerability affecting the LiteSpeed cPanel plugin to its Known Exploited Vulnerabilities catalog. The flaw, tracked as CVE-2026-54420, centers around improper symlink handling and weak privilege assignment policies inside the plugin's architecture. Threat actors are actively exploiting this bug on web hosting servers to elevate their access from standard local users directly to full root administrative authority, completely compromising the underlying web infrastructure.

Attack Type : Privilege Escalation to Root

Root Cause : Improper Symlink Handling

The Bottom Line : Update the LiteSpeed cPanel plugin to the latest version and enforce strict local system access boundaries.

17. Security Gateways Under Fire: FortiSandbox Flaws Enable Authentication Bypass

An active cyber campaign has been detected targeting security analysis infrastructure. Threat actors are chaining together three distinct vulnerabilities inside Fortinet FortiSandbox appliances. By combining improper input validation bugs with operating system command injection flaws, remote attackers can bypass local authentication mechanisms entirely. This allows them to execute arbitrary system commands with elevated privileges, turning an organization's malware analysis sandbox into a primary pivot point into the internal network.

Attack Type : Auth Bypass / OS Command Injection

Root Cause : Improper Input Validation

The Bottom Line : Isolate sandbox analysis appliances on dedicated VLANs and apply Fortinet's June firmware updates.

18. Squidbleed Flaw Exposes Enterprise Proxy Memory Secrets

A critical memory-disclosure vulnerability, dubbed Squidbleed and tracked as CVE-2026-47729, has been uncovered in the widely used Squid Proxy software. The flaw resides within the proxy's FTP protocol parsing architecture, which fails to execute proper null-terminator boundary checks during data processing. Remote attackers can intentionally feed malformed FTP requests into the proxy, triggering a memory leak that forces the application to return raw snippets of adjacent system memory, potentially exposing sensitive session tokens, credentials, and cross-tenant corporate web traffic.

Attack Type : Memory Disclosure

Root Cause : FTP Parsing Null Check Missing

The Bottom Line : Patch active Squid Proxy deployments immediately and restrict legacy FTP traffic routing through proxies.

19. FortiBleed Incident Exposes Credentials for Tens of Thousands of Edge Devices

An extensive credential exposure event, known as FortiBleed, has created significant risk across global corporate perimeters. Security researchers discovered that due to widespread systemic password reuse and weak administrative security hygiene, credentials for roughly 73,000 Fortinet network edge appliances have been leaked or brute-forced online. Threat actors are actively weaponizing this credential list to log directly into enterprise VPN gateways, bypass external firewalls, and establish immediate corporate network footholds.

Attack Type : Credential Exposure / Brute Force

Root Cause : Credential Reuse and Hygiene

The Bottom Line : Enforce global password resets for all firewall administrators and mandate multi-factor authentication on all perimeters.

20. AryStinger Botnet Enters Legacy Routers into Cyber Recon Army

Threat actors have compiled a large-scale router botnet named AryStinger by targeting unpatched hardware at the perimeter. The botnet has successfully ensnared over 4,300 legacy D-Link routers that have reached end-of-life status and no longer receive official security patches. The attackers exploit known vulnerabilities to compromise these edge devices, converting them into a distributed, anonymous reconnaissance proxy network used to hide the origin of active cyberattacks against corporate and government targets.

Attack Type : Router Botnet / Proxy Network

Root Cause : Outdated Unpatched Routers

The Bottom Line : Decommission end-of-life network equipment and isolate edge devices from the public internet.

PRODUCT LAUNCH 2026

BriskInfosec™
VULNERABILITY TO VICTORY

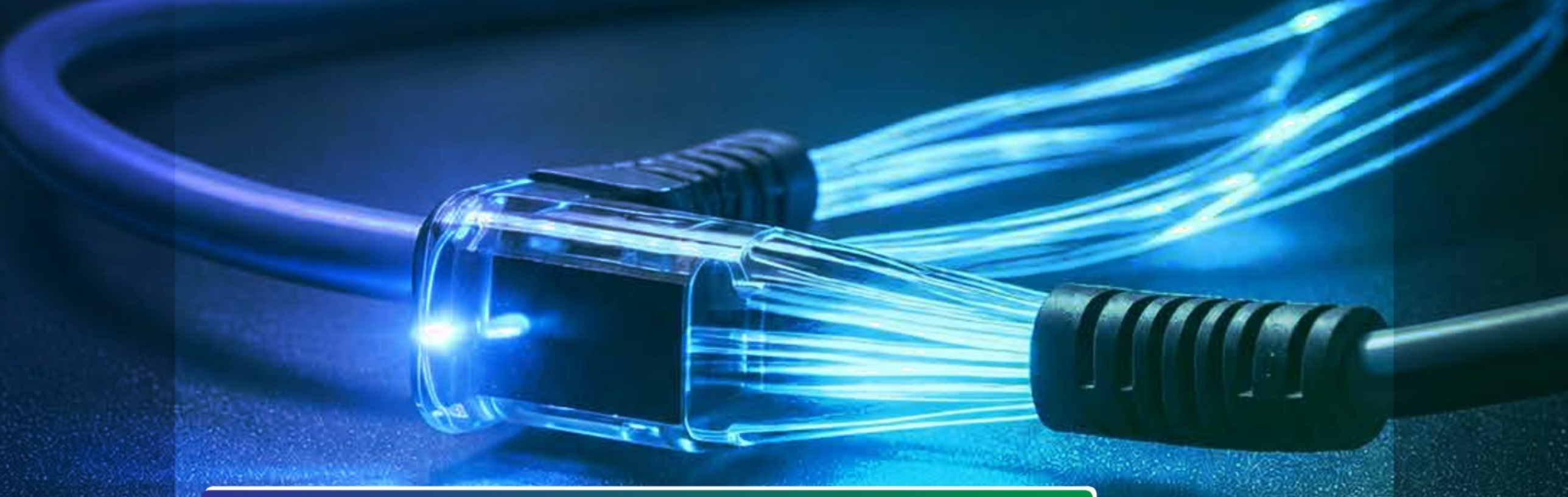
luraInsight

Offline SAST for Enterprise

Offline AI-Powered Static Application Security Testing

YOUR CODE. YOUR NETWORK. YOUR CONTROL

100% OFFLINE	OWN AI MODEL	ALL-IN-ONE APPSEC	DEEP STATIC ANALYSIS
Zero data exposure	Built for secure code review	SAST, SCA, SBOM & CBOM	Accurate vulnerability detection



PART OF THE BRISKINFOSEC CYBERSECURITY ECOSYSTEM

LURA PORTAL | VAPT | BSOC | COMPLIANCE | LURAINSIGHT

Experience LuraInsight

CREST Accredited | CERT-In Empanelled | ISO 27001 Certified

AI and Modern Application Vulnerabilities

21. ShinyHunters Leverages Unauth Oracle PeopleSoft Flaw to Breach Universities

The notorious cybercrime group ShinyHunters successfully targeted multiple higher education institutions by exploiting a zero-day vulnerability in Oracle PeopleSoft. Tracked as CVE-2026-35273, the flaw exists within the Oracle PeopleSoft Environment Management Hub (PSEMHUB), which completely lacks proper authentication checks for specific administrative requests. This allows remote, unauthenticated attackers to execute arbitrary code across backend environments, providing direct access to student databases, proprietary financial systems, and internal academic data.

Attack Type : Unauthenticated RCE

Root Cause : Missing Authentication in PSEMHUB

The Bottom Line : Restrict PeopleSoft PSEMHUB access behind enterprise VPNs and apply vendor patches immediately.

22. Actively Exploited Splunk Enterprise Pre-Auth RCE Demands Immediate Patching

CISA has issued an urgent directive mandating federal agencies and private sector partners to secure their log management infrastructure. A critical pre-authentication remote code execution vulnerability, tracked as CVE-2026-20253, is being actively exploited in Splunk Enterprise. The flaw represents a severe missing authentication check (CWE-306) within specific web components, enabling remote threat actors to run malicious commands on the host server without providing valid credentials, threatening the integrity of enterprise security telemetry.

Attack Type : Unauthenticated RCE

Root Cause : Missing Authentication

The Bottom Line : Patch Splunk instances immediately and limit administrative port exposure to trusted internal networks.

23. CISA Issues Urgent Mandate to Patch Max Severity Joomla Content Editor Flaw

A maximum-severity vulnerability affecting the Joomla Content Editor component has triggered an emergency patch mandate from CISA. The flaw, tracked as CVE-2026-48907, scores a maximum CVSS rating due to an improper access control failure (CWE-284). Remote, unauthenticated attackers are actively exploiting this security hole on public-facing web servers to upload malicious scripts and execute arbitrary PHP code, giving them the ability to entirely deface, wipe, or compromise underlying web application hosts.

Attack Type : Arbitrary PHP Code Execution

Root Cause : Improper Access Control

The Bottom Line : Update Joomla Content Editor extensions instantly and implement a robust web application firewall.

24. WordPress Gravity SMTP Plugin Infiltration Spikes in June

Automated botnets are conducting widespread campaigns targeting the WordPress ecosystem by focusing on the Gravity SMTP plugin. The zero-day flaw, tracked as CVE-2026-4020, stems from an unprotected REST API endpoint that completely fails to validate user privileges. Threat actors can query this open endpoint to trigger unauthenticated information disclosure, downloading internal system configuration details, mail server passwords, and database connection strings to facilitate complete site takeovers.

Attack Type : Unauthenticated Information Disclosure

Root Cause : Unprotected REST API Endpoint

The Bottom Line : Disable unused REST API endpoints and verify that the Gravity SMTP plugin is running the latest version.

25. Microsoft Validates RoguePlanet Defender Zero Day Privilege Escalation Flaw

Microsoft has officially confirmed the existence of an actively exploited zero-day vulnerability within the core Windows Defender security engine. Tracked as CVE-2026-50656 and dubbed RoguePlanet, the flaw involves a classic race condition bug occurring during local file analysis. A public proof-of-concept (PoC) exploit has been released online. Local threat actors or low-privilege malware strains can exploit this race condition to escalate their access to full system-level administrative privileges, effectively disabling Windows Defender protections from within.

Attack Type : Local Privilege Escalation

Root Cause : Race Condition in Defender Engine

The Bottom Line : Monitor for rapid, anomalous local file creation patterns and deploy the latest Microsoft endpoint definitions.

26. Unpatchable usbliter8 BootROM Exploit PoC Surfaces for Older Apple Silicon

An immutable security hardware defect has resurfaced following the public release of a functional proof-of-concept exploit named usbliter8. This flaw targets the physical BootROM architecture embedded inside older Apple A12 and A13 Bionic silicon chips. Because the BootROM code is written directly into the chip fabrication hardware, it cannot be modified or patched via software updates. Threat actors with direct, physical access to a target device can exploit this flaw via USB to execution-lock the device and run untrusted, custom code beneath the operating system layers.

Attack Type : BootROM Exploit

Root Cause : SecureROM Flaw Physical Access

The Bottom Line : Implement strict physical device security controls and mandate corporate device replacement for deprecated silicon hardware.

27. Microsoft Fixes Hundreds of Flaws in June Patch Tuesday While Introducing OS Bugs

Microsoft's June 2026 Patch Tuesday rollout has created significant operational challenges for IT and security departments worldwide. While the massive monthly security update resolved a record-breaking 208 distinct vulnerabilities spanning the Windows portfolio, the update package simultaneously introduced a severe regression bug. Upon installation, the patch unexpectedly breaks the core Windows Recycle Bin application functionality, forcing system administrators to choose between maintaining critical flaw mitigations or risking local operating system instability.

Attack Type : Multiple Security Mitigations

Root Cause : Monthly Rollup with Regression Bug

The Bottom Line : Stage and test large-scale monthly rollups on pilot groups before pushing updates to production systems.

28. AutoJack Chains Prompt Injection with Localhost Flaws for Remote Code Execution

The rapid enterprise adoption of autonomous artificial intelligence has introduced a critical new exploit vector named AutoJack. Security researchers proved that a user visiting a malicious web page can inadvertently trigger an exploit chain targeting Microsoft's AutoGen Studio framework running locally. The attack relies on an advanced prompt injection that tricks the AI agent into executing commands. Because AutoGen Studio operates an unauthenticated localhost background service, the injected prompt can successfully pivot to execute malicious code directly on the user's host computer.

Attack Type : Agent Hijack / Remote Code Execution

Root Cause : Prompt Injection LocalhostSvc

The Bottom Line : Bind AI framework local services strictly to local loopback adapters and sanitize all dynamic agent inputs.

29. Pickle in the Middle Flaw in Google Vertex AI SDK Allows Model Upload Manipulation

A serious security vulnerability termed Pickle in the Middle has been identified inside the Google Vertex AI SDK. The flaw combines cloud bucket squatting risks with unsafe data deserialization practices during the machine learning model creation process. Threat actors can exploit this vulnerability to intercept and hijack machine learning model uploads. By swapping legitimate model files with trojanized objects utilizing unsafe Python pickle formatting, the attackers can achieve full remote code execution when the model is subsequently parsed by developer teams or automated AI production pipelines.

Attack Type : Model-Upload Hijack / Code Execution

Root Cause : Bucket Squatting Deserialization

The Bottom Line : Disallow unsafe pickle deserialization in ML workflows and enforce cryptographically signed model verification.

WE ARE EXHIBITING AT

GISEC GLOBAL 2026

We are pleased to announce our participation in GISEC GLOBAL 2026, the Middle East's premier cybersecurity event.

Change to Visit our booth to meet our cybersecurity experts, discuss your security challenges, and explore our latest cybersecurity solutions.

September 16–18, 2026

Dubai Exhibition Centre, Expo City

Hall 4 – E90

We look forward to connecting with industry leaders, partners, and security professionals from around the world.

See you at GISEC GLOBAL 2026!

HOPE IS NOT A CYBERSECURITY STRATEGY. RESILIENCE IS.

BriskInfosec™
VULNERABILITY TO VICTORY

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