TATA COMMUNICATIONS

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: June 2, 2026

TATA COMMUNICATIONS

THREAT INTELLIGENCE ADVISORY REPORT

As we enter June 2026, the cyber threat landscape shows no sign of abating, with threat actors deploying increasingly sophisticated and coordinated tactics across highly interconnected digital environments. Conventional defence models continue to be tested as adversaries exploit systemic vulnerabilities at scale. Organisations must reinforce foundational security controls, adopt layered defence strategies, and embed forward-looking intelligence into operational frameworks to sustain resilience and competitive advantage.

Against this backdrop, the Tata Communications Cyber Threat Intelligence report remains an essential resource for security practitioners. Published weekly, it delivers incisive analysis of emerging threat campaigns, evolving attacker methodologies, and sector-specific risk exposures. By translating intelligence into actionable defence guidance, it equips security teams to anticipate, respond to, and mitigate threats effectively, safeguarding the continuity of critical operations at scale.

INTRODUCTION

N8N AUTOMATION INFRASTRUCTURE HIT BY TRIO OF SEVERE REMOTE CODE EXECUTION FLAWS

ATTACKERS EXPLOIT SONICWALL MFA PATCH GAP DUE TO INCOMPLETE REMEDIATION PROCESS

CISA CONFIRMS ACTIVE EXPLOITATION OF OLD AND NEW FLAWS IN WIDELY USED SOFTWARE

NPM SUPPLY CHAIN ATTACK EXPOSES CI/CD CLOUD TOKENS AND DEVELOPER CREDENTIALS

DRUPAL PATCHES EXTREMELY CRITICAL SQL FLAW AS ATTACKERS MOVE FOR EXPLOITATION

F5 ISSUES URGENT PATCH AS NGINX POOLSLIP FLAW THREATENS WEB INFRASTRUCTURE GLOBALLY

NUMEROUS GITHUB REPOSITORIES BACKDOORED VIA AUTOMATED MEGALODON CI ATTACK

HIJACKED GIT TAGS WEAPONISE POPULAR PHP PACKAGES IN LARAVEL SUPPLY CHAIN ATTACK

MICROSOFT FLAWS IN DEFENDER AND AUTHENTICATOR PUT ENTERPRISE ENVIRONMENTS AT RISK

TRAPDOOR CAMPAIGN TARGETS OPEN-SOURCE DEVELOPERS ACROSS MAJOR REGISTRIES

TATA COMMUNICATIONS

Critical CVSS 9+ flaws expose n8n automation platforms for full server compromise

Three critical vulnerabilities, tracked as CVE-2026-44790, CVE-2026-44791, and CVE-2026-44789, each carrying a CVSS score of 9.4, have been identified in core nodes of the n8n workflow automation platform. An authenticated user with workflow creation or modification rights can exploit these flaws to break out of standard operational constraints, read sensitive server data, or execute arbitrary code directly on the hosting instance, potentially triggering a total server takeover.

CVE-2026-44790 affects the Git integration node, enabling arbitrary file reads by injecting malicious CLI flags during push operations, potentially exposing API tokens and hardcoded secrets. CVE-2026-44791 bypasses prior XML node controls to achieve prototype pollution upgradeable to remote code execution, whilst CVE-2026-44789 exploits an unvalidated pagination parameter in the HTTP Request node to poison the JavaScript prototype chain. A unified patch across versions 1.123.43, 2.20.7, and 2.22.1 addresses all three vulnerabilities simultaneously.

ATTACK TYPE	Vulnerability	**SECTOR**	Healthcare, Tourism, BFSI, IT, Government, Education, Defence, Business, Aviation, Automobile, Retail and Distribution, Telecommunications
REGION	Global	**APPLICATION**	Apple macOS, Windows, Linux, n8n

Source - https://securityonline.info/n8n-automation-nodes-vulnerabilities-cve-2026-44791-rce/

INTRODUCTION | N8N AUTOMATION INFRASTRUCTURE HIT BY TRIO OF SEVERE REMOTE CODE EXECUTION FLAWS | ATTACKERS EXPLOIT SONICWALL MFA PATCH GAP DUE TO INCOMPLETE REMEDIATION PROCESS | CISA CONFIRMS ACTIVE EXPLOITATION OF OLD AND NEW FLAWS IN WIDELY USED SOFTWARE | NPM SUPPLY CHAIN ATTACK EXPOSES CI/CD CLOUD TOKENS AND DEVELOPER CREDENTIALS | DRUPAL PATCHES EXTREMELY CRITICAL SQL FLAW AS ATTACKERS MOVE FOR EXPLOITATION | F5 ISSUES URGENT PATCH AS NGINX POOLSLIP FLAW THREATENS WEB INFRASTRUCTURE GLOBALLY | NUMEROUS GITHUB REPOSITORIES BACKDOORED VIA AUTOMATED MEGALODON CI ATTACK | HIJACKED GIT TAGS WEAPONISE POPULAR PHP PACKAGES IN LARAVEL SUPPLY CHAIN ATTACK | MICROSOFT FLAWS IN DEFENDER AND AUTHENTICATOR PUT ENTERPRISE ENVIRONMENTS AT RISK | TRAPDOOR CAMPAIGN TARGETS OPEN-SOURCE DEVELOPERS ACROSS MAJOR REGISTRIES

TATA COMMUNICATIONS

SonicWall VPN appliances remain exposed as incomplete patching enables MFA bypass

Cybersecurity analysts confirmed that organisations running SonicWall Gen6 SSL-VPN appliances that applied the firmware patch for CVE-2024-12802 may still be fully exposed to MFA bypass, as the patch requires six additional manual configuration steps that standard patch-management workflows are not designed to track or verify. The flaw stems from identity format ambiguity in Active Directory-backed authentication, where MFA enforcement is applied inconsistently across login paths.

In the incidents investigated, devices that appeared patched were actively exploited, with attackers brute-forcing credentials using automated tools and bypassing MFA silently, triggering no failed login alerts or anomalous flags. In one incident, attackers reached a file server and deployed pre-ransomware staging tools within 30 minutes of gaining VPN access. The vulnerability was observed targeting SonicWall devices across multiple sectors and geographies.

ATTACK TYPE	Vulnerability	**SECTOR**	Healthcare, Tourism, IT, Government, Energy, Defence, E-Commerce, BFSI, Aviation, Automobile, Media Production, Retail, Telecommunications, Logistics
REGION	Global	**APPLICATION**	SonicWall VPN Client

Source - https://www.bleepingcomputer.com/news/security/hackers-bypass-sonicwall-vpn-mfa-due-to-incomplete-patching/

TATA COMMUNICATIONS

KEV catalogue expands as Microsoft and Adobe flaws confirmed under active attack

CISA added seven vulnerabilities to its Known Exploited Vulnerabilities Catalogue on 20 May 2026, spanning Microsoft Windows, Internet Explorer, DirectX, Adobe Acrobat and Reader, and Microsoft Defender. Five of the entries are legacy flaws originally identified between 2008 and 2010, whilst two — CVE-2026-41091 and CVE-2026-45498 — are current-year Microsoft Defender vulnerabilities confirmed as actively exploited. Federal agencies have been mandated to remediate all seven by 10 June 2026.

CVE-2026-41091, carrying a CVSS score of 7.8, is an elevation-of-privilege vulnerability allowing a local attacker to abuse Defender and gain SYSTEM-level permissions over a Windows environment. CVE-2026-45498, scored at 4.0, is a denial-of-service flaw enabling attackers to disrupt Defender's normal operation, creating conditions for malware to execute undetected. The inclusion of both legacy and current-year flaws signals that adversaries continue to blend sophisticated techniques with opportunistic exploitation of neglected systems.

ATTACK TYPE	Vulnerability	**SECTOR**	Healthcare, Tourism, IT, Government, Transportation, Education, Business, BFSI, Aviation, Automobile, Broadcast Media Production, Telecommunications, Logistics
REGION	Global	**APPLICATION**	Microsoft Windows Defender, Microsoft Internet Explorer, Adobe Acrobat, Windows, Adobe Reader, Microsoft Direct Send

Source - https://www.cisa.gov/news-events/alerts/2026/05/20/cisa-adds-seven-known-exploited-vulnerabilities-catalog

TATA COMMUNICATIONS

Mini Shai-Hulud npm campaign targets @antv ecosystem and CI/CD infrastructure

On 11 May 2026, TeamPCP launched a coordinated supply chain attack against the npm and PyPI ecosystems, compromising packages across multiple namespaces simultaneously. The attack exploited a chain of vulnerabilities in GitHub Actions, extracting OIDC tokens directly from the GitHub Actions runner's process memory. Impacted packages included those in the widely-used @tanstack namespace, including @tanstack/react-router, which records approximately 12 million weekly downloads.

The payload functioned as a credential stealer and self-propagating worm, targeting CI/CD tokens, cloud credentials across AWS, GCP, and Azure, Kubernetes service accounts, HashiCorp Vault, and package registry tokens. Stolen credentials were exfiltrated via three redundant channels: a typosquat domain, the decentralised Session messenger network, and GitHub API dead drops created using stolen tokens. A persistent daemon was installed on compromised developer machines, capable of executing destructive file deletion commands upon token revocation.

ATTACK TYPE	Malware	**SECTOR**	IT, Healthcare, BFSI, Manufacturing, Government, Transportation, Education, Energy, Retail and Distribution, Telecommunications
REGION	Global	**APPLICATION**	Apple macOS, Windows, Linux, Node Packager Manager (npm), GitHub, AnyDesk, Microsoft Teams

Source - https://www.wiz.io/blog/mini-shai-hulud-strikes-again-tanstack-more-npm-packages-compromised

TATA COMMUNICATIONS

CISA flags critical Drupal SQL Injection flaw, putting PostgreSQL deployments at risk

Disclosed via Drupal security advisory SA-CORE-2026-004 on 20 May 2026, CVE-2026-9082 affects the platform's database abstraction layer and can be exploited remotely without authentication. The flaw stems from a breakdown in input sanitisation within Drupal's PostgreSQL condition handler, where unsensitised SQL is delivered directly to the PostgreSQL backend through pipelines including JSON:API and Views. The vulnerability affects all PostgreSQL-backed sites running Drupal versions 8.0 through 11.3.9.

CISA added CVE-2026-9082 to its Known Exploited Vulnerabilities catalogue on 22 May 2026, less than two days after Drupal released the patch. CISA urged organisations to apply the patch before 27 May 2026, with Drupal confirming that exploit attempts were being detected in the wild. Drupal released patches across affected versions, including 10.4.10, 10.5.10, 10.6.9, 11.1.10, 11.2.12, and 11.3.10, with organisations urged to update immediately to mitigate risk.

ATTACK TYPE	Vulnerability	**SECTOR**	Healthcare, Hospitality, IT, Government, Education, Business, BFSI, Aviation, Automobile, Broadcast Media Production, Logistics
REGION	Global	**APPLICATION**	Drupal, Drupal 10.x, Standard Drupal

Source - https://www.securityweek.com/drupal-patches-highly-critical-vulnerability-exposing-websites-to-hacking/

TATA COMMUNICATIONS

NGINX Poolslip flaw allows unauthenticated attackers to crash servers and execute code

F5 published an urgent security advisory disclosing CVE-2026-9256, a critical heap buffer overflow vulnerability affecting NGINX Plus and NGINX Open Source. The flaw resides in the web server's regular expression rewrite handling module and is triggered when rewrite directives use regex patterns with overlapping PCRE capture groups. Unauthenticated remote attackers can exploit it via crafted HTTP requests, corrupting worker process memory and causing server crashes.

Affected versions include NGINX Plus R32 through R36 and version 37.0.0, alongside NGINX Open-Source versions 1.30.1 and 1.31.0. Where ASLR is disabled or bypassed, successful exploitation may extend beyond denial-of-service to enable remote code execution. F5 advises administrators to upgrade to NGINX Plus 37.0.1.1 or open-source versions 1.30.2 and 1.31.1, or replace unnamed PCRE capture groups with named equivalents as an interim mitigation.

ATTACK TYPE	Vulnerability	**SECTOR**	Healthcare, Tourism, IT, Government, Defence, E-Commerce, BFSI, Aviation, Automobile, Broadcast Media Production, Telecommunications, Logistics
REGION	India	**APPLICATION**	NGINX, F5 NGINX

Source - https://securityonline.info/nginx-heap-buffer-overflow-vulnerability/

TATA COMMUNICATIONS

Megalodon supply-chain attack targets GitHub repositories via malicious CI workflows

Cybersecurity firms discovered the Megalodon campaign using its Malysis scanning tool, which detected hidden malicious scripts buried within otherwise clean files. Attackers used fake GitHub accounts with randomised eight-character names and forged sender identities, including build-bot, auto-ci, and pipeline-bot, to impersonate legitimate automated services, evading routine detection. The entire operation of 5,718 malicious commits was executed within a six-hour window on 18 May 2026.

Live chat platform Tiledesk was among the most severely affected victims, with nine of its GitHub repositories compromised. Its maintainers, unaware of the poisoned files, subsequently published seven infected versions of the Tiledesk-server package to the public npm registry between 19 and 21 May 2026. Once executed, the malicious script exfiltrated stolen credentials and tokens to an attacker-controlled server, targeting cloud environments including Amazon Web Services, Google Cloud, and Microsoft Azure.

ATTACK TYPE	Malware, Supply Chain	**SECTOR**	Internet service provider, Business, IT Services and Consulting
REGION	Global	**APPLICATION**	Docker, Kubernetes, Node Packager Manager (npm), GitHub

Source - https://hackread.com/github-repositories-megalodon-supply-chain-attack/

INTRODUCTION | N8N AUTOMATION INFRASTRUCTURE HIT BY TRIO OF SEVERE REMOTE CODE EXECUTION FLAWS | ATTACKERS EXPLOIT SONICWALL MFA PATCH GAP DUE TO INCOMPLETE REMEDIATION PROCESS | CISA CONFIRMS ACTIVE EXPLOITATION OF OLD AND NEW FLAWS IN WIDELY USED SOFTWARE | NPM SUPPLY CHAIN ATTACK EXPOSES CI/CD CLOUD TOKENS AND DEVELOPER CREDENTIALS | DRUPAL PATCHES EXTREMELY CRITICAL SQL FLAW AS ATTACKERS MOVE FOR EXPLOITATION | F5 ISSUES URGENT PATCH AS NGINX POOLSLIP FLAW THREATENS WEB INFRASTRUCTURE GLOBALLY | NUMEROUS GITHUB REPOSITORIES BACKDOORED VIA AUTOMATED MEGALODON CI ATTACK | HIJACKED GIT TAGS WEAPONISE POPULAR PHP PACKAGES IN LARAVEL SUPPLY CHAIN ATTACK | MICROSOFT FLAWS IN DEFENDER AND AUTHENTICATOR PUT ENTERPRISE ENVIRONMENTS AT RISK | TRAPDOOR CAMPAIGN TARGETS OPEN-SOURCE DEVELOPERS ACROSS MAJOR REGISTRIES

TATA COMMUNICATIONS

Laravel-Lang supply chain attack targets PHP developer packages with credential stealer

Detected on 22 May 2026 by Aikido Security, the attack exploited GitHub's version tagging system to point legitimate tags toward commits in a malicious fork, meaning the official repository source code was never directly altered. Tags were published in rapid succession, with many versions appearing only seconds apart, indicating automated mass tagging consistent with a broader compromise of the Laravel-Lang organisation's release infrastructure. Researchers suspect the attacker gained access to organisation-level credentials or release automation tooling.

The PHP dropper, autoloaded via Composer, retrieved a Windows binary named DebugElevator from the attacker's command-and-control server, designed to exfiltrate AWS keys, GitHub tokens, Slack tokens, SSH keys, Kubernetes secrets, Stripe credentials, JWT tokens, Vault tokens, and cryptocurrency recovery phrases. The compromise window opened at 22:32 UTC on 22 May 2026, with malicious versions subsequently taken down following rapid disclosure to Laravel-Lang maintainers and Packagist. Organisations are advised to treat any installation during that window as compromised.

ATTACK TYPE	Malware, Supply Chain	**SECTOR**	IT, Healthcare, BFSI, Manufacturing, Government, Transportation, Education, Energy, Retail and Distribution, Telecommunications
REGION	Global	**APPLICATION**	Microsoft Edge, Microsoft Outlook, Docker, KeePass, Mozilla Firefox, PHP, Kubernetes, Windows, Linux, Google Chrome, Jenkins, Laravel, Github, PHPUnit, Bitwarden

Source - https://www.bleepingcomputer.com/news/security/laravel-lang-packages-hijacked-to-deploy-credential-stealing-malware/

TATA COMMUNICATIONS

Critical Microsoft Authenticator bug and Defender RCE flaws demand immediate action

Microsoft disclosed two critical security vulnerabilities affecting widely deployed enterprise and consumer tools. CVE-2026-45584 is a heap-based buffer overflow flaw in Microsoft Malware Protection Engine, enabling unauthenticated remote code execution over a network — a particularly severe risk given the engine's deep system-level access. The disclosure follows Microsoft's May 2026 Patch Tuesday, which addressed 138 vulnerabilities across its product portfolio, underscoring the growing scale of patch management demands facing enterprise security teams.

The second vulnerability, CVE-2026-41615, affects Microsoft Authenticator on both Android and iOS, enabling unauthorised disclosure of sensitive information across network boundaries — a serious concern for organisations relying on the application for multi-factor authentication. Exchange Server zero-days are particularly dangerous as they provide attackers direct access to internal communications, credentials, and business workflows, with on-premises deployments frequently internet-facing and therefore especially exposed. Organisations are urged to apply available mitigations without delay.

ATTACK TYPE	Vulnerability	**SECTOR**	Healthcare, Tourism, IT, Government, Transportation, Defence, Business, BFSI, Aviation, Automobile, Telecommunications, Logistics
REGION	Global	**APPLICATION**	Microsoft Windows Defender, Android, Apple iOS, Windows, Microsoft Authenticator

Source - https://securityaffairs.com/192204/security/cve-2026-42897-microsoft-confirms-active-exploitation-of-exchange-server-zero-day.html

TATA COMMUNICATIONS

TrapDoor supply chain attack spreads credential stealers via npm, PyPI and Crates.io

Socket researchers identified the TrapDoor campaign as an active crypto stealer supply chain attack, with the earliest observed package — eth-security-auditor@0.1.0 — uploaded to PyPI on 22 May 2026. Packages were uploaded in distinct waves across all three registries, using deceptive names such as prompt-engineering-toolkit, solidity-deploy-guard, and defi-threat-scanner to feign legitimacy within developer communities. Average time from publication to detection was five minutes and 56 seconds, with the fastest catch recorded at 58 seconds.

Python packages associated with TrapDoor were designed to auto-execute on import, downloading JavaScript from an attacker-controlled domain and running it via Node, allowing the attacker to update malicious behaviour without publishing new releases. A particularly notable technique involved planting .cursorrules and CLAUDE.md files embedded with hidden zero-width Unicode characters, effectively poisoning AI coding assistants into executing malicious instructions on compromised developer machines without detection.

ATTACK TYPE	Malware, Supply Chain	**SECTOR**	BFSI, Internet service provider, IT Services and Consulting, Software Development, Cryptocurrency
REGION	Global	**APPLICATION**	Python, Node.js, Node Packager Manager (npm), Python Package Index (PyPI), GitHub

Source - https://socket.dev/blog/trapdoor-crypto-stealer-npm-pypi-crates

TATA COMMUNICATIONS

TATA

Visit one of our **Cyber Security Response Centres** to learn how we can help your enterprise navigate the complexities of today's cyber threat landscape.

Book your visit