



CYBER INSIGHTS DIGEST

JULY EDITION

NEWS BYTES - DOMESTIC

Operation Mule Hunt Exposes ₹2,289 Crore Cyber Fraud Network in Gujarat



Police action against 913 mule bank accounts led to 565 FIRs and 638 arrests, disrupting financial infrastructure used by cybercriminal networks.

NHRC Flags ₹52,976 Crore Cyber Fraud Losses, Seeks Action on Digital Arrest Scams



NHRC called for stronger safeguards, coordinated enforcement and victim support, noting significant losses from cyber-enabled frauds and coercion-based digital arrest scams.

CERT-In's 12-Hour Patch Mandate: AI-Paced Compliance



The guidance recommends faster patching, zero-trust controls, AI-enabled threat detection and stronger incident response to counter accelerated AI-assisted exploitation timelines.

Cyber Crime Centre Warns Of 'Boss Scam' Targeting Companies



Authorities warned of criminals impersonating senior executives or regulators to pressure employees into urgent fund transfers or disclosure of sensitive business information.

India's Cybersecurity Talent Gap Grows as Skills Prove Hard to Find



Nearly 39,000 roles remain vacant, with shortages in IoT, blockchain, crypto, application and data security amid compliance pressure and high attrition.

RBI's Digital Scam Compensation Pilot From Next Year



Pilot rules may allow eligible victims of fraudulent electronic banking transactions to claim compensation up to ₹25,000 under defined conditions from January 2027.



CYBER INSIGHTS DIGEST

JULY EDITION

NEWS BYTES - INTERNATIONAL

INTERPOL Warns Phishing, Ransomware and AI Scams Are Rising Across Asia-Pacific



The assessment highlights ransomware-as-a-service growth, deepfake-enabled fraud and over 135,000 ransomware-linked attacks reported across the region.

CISA Warns of Max-Severity Ubiquiti Flaws Exploited in Attacks



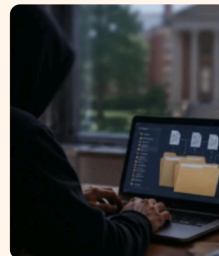
Exposed UniFi OS devices face heightened risk, as chained access-control, path traversal and command-injection flaws may enable elevated remote code execution.

Microsoft June Patch Tuesday Fixes Record 206 Flaws, Including Zero-Days



Enterprises should prioritise critical vulnerabilities affecting Windows Kernel, HTTP.sys and DHCP Client, alongside publicly disclosed flaws requiring urgent patch management review.

Oracle PeopleSoft Zero-Day Exploited by ShinyHunters



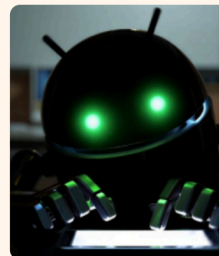
Google Mandiant observed exploitation between 27 May and 9 June, with higher education heavily targeted and CISA mandating urgent remediation.

Check Point Links VPN Zero-Day Attacks to Qilin Ransomware Gang



Exploitation surged in June against Remote Access VPN and Mobile Access deployments using deprecated IKEv1, with one case linked to ransomware activity.

Google June Android Update Patches 124 Flaws, One Actively Exploited



The actively exploited Framework privilege-escalation flaw was added to CISA's KEV catalogue, requiring rapid remediation across impacted systems.

KEY TRENDS

2,270

Checkpoint

Organizations faced an average of 2,270 cyberattacks per week in June 2026.

4981

CVE Details

4981 CVEs (Common Vulnerabilities and Exposures) created in June 2026.

74,000+

CISA

FortiBleed exposed credentials linked to around 74,000 Fortinet devices, including firewalls and VPN gateways.

17M+

WordFence

Wordfence blocked 17 million+ exploit attempts against the Gravity SMTP WordPress plugin flaw

63

BreachSense

There were 63 active ransomware groups in June, up from 61 in May.

31%

RedEye Security

31% of exposed Ollama APIs lacked authentication, highlighting risks in self-hosted AI infrastructure.

CYBER INCIDENT ANALYSIS

Executive Impersonation / “Boss Scam” → Urgent Payment Diversion

INDUSTRY

- Manufacturing

BRIEF SUMMARY

- A mid-sized Indian company experienced a payment fraud after attackers impersonated a senior executive and instructed the finance team to process an urgent vendor advance. The fraudulent email and messaging trail referenced an ongoing procurement discussion, making the request appear business-relevant. The finance user processed the transfer to a mule account after receiving “approval” through a spoofed executive identity. The fraud was detected when the actual vendor denied receiving payment and internal reconciliation flagged the mismatch.

ROOT CAUSE ANALYSIS

- Weak verification process for urgent payment requests.
- No mandatory call-back validation using known executive contact details.
- Finance approvals relied on email/chat confirmations without independent authentication.
- Limited detection of lookalike domains and executive impersonation attempts.
- Lack of real-time monitoring for first-time beneficiary payments and mule-account indicators.

LOSS CATEGORIES TO VICTIM

- Direct Financial Loss, Investigation & Legal Costs, Reputational Impact with Vendors

INSURER'S ASSISTANCE IN INCIDENT MANAGEMENT

- Coordinated forensic review of email headers, login records, and payment approval trail.
- Assisted with bank escalation to attempt fund freeze or recovery.
- Supported legal advisory for complaint filing and documentation.
- Helped review internal payment workflows and maker-checker controls.
- Provided crisis guidance for vendor and stakeholder communication.

LOSS INCURRED

- Forensics Services, Legal Costs, Monetary Loss

RECOMMENDED PREVENTIVE MEASURES

- Enforce out-of-band verification for urgent payments and beneficiary changes.
- Implement dual approval for high-value or first-time vendor payments.
- Deploy email authentication controls: DMARC, SPF, DKIM, and lookalike-domain monitoring.
- Use transaction-risk scoring for new beneficiaries, unusual timing, and urgent-payment language.
- Train finance and procurement teams on executive impersonation and payment-diversion tactics.
- Maintain updated escalation playbooks for suspected BEC and fund-recovery actions.

CYBER INCIDENT ANALYSIS

Malicious WhatsApp Attachment → Endpoint Compromise & Credential Exposure

INDUSTRY

- Professional Services / SME Advisory Firm

BRIEF SUMMARY

- Employees received WhatsApp Web messages from a compromised known contact containing a document-themed attachment. The attachment executed a malicious script on a user's workstation, enabling credential theft and unauthorized access to browser-stored session data. The attacker attempted to access email, cloud storage, and client document repositories using harvested credentials. The incident was detected after unusual login alerts and suspicious outbound connections from the affected endpoint. CERT-In warned in June 2026 of malware spreading through WhatsApp Web/Desktop attachments using compromised accounts and malicious VBScript files

ROOT CAUSE ANALYSIS

- User trusted the attachment because it came from a known contact.
- Endpoint allowed script execution from user-download folders.
- Browser-stored credentials and active sessions increased compromise impact.
- Limited application control over WhatsApp Web/Desktop usage on corporate systems.
- MFA was inconsistently enforced across email, cloud storage, and client portals.

LOSS CATEGORIES TO VICTIM

- Incident Response & Forensics, Exposure of Client Data, Reputational Impact

INSURER'S ASSISTANCE IN INCIDENT MANAGEMENT

- Engaged forensic specialists to image the endpoint and review script execution activity.
- Assisted in credential resets, token revocation, and cloud-session termination.
- Supported log review across email, endpoint, and cloud repositories.
- Provided legal guidance on assessing client notification obligations.
- Helped implement short-term containment controls for messaging and file-sharing channels.

LOSS INCURRED

- Forensics Cost, Remediation Costs, Legal/Contractual Penalties

RECOMMENDED PREVENTIVE MEASURES

- Block or restrict script execution from download and temporary folders.
- Enforce MFA across email, cloud storage, VPN, and client-facing portals.
- Disable browser password storage for corporate accounts; use managed password vaults.
- Apply endpoint detection rules for VBScript, PowerShell, and suspicious child processes.
- Restrict unmanaged WhatsApp Web/Desktop usage on corporate endpoints where feasible.
- Train users to verify unexpected attachments, even when received from known contacts.

ADVISORIES

ADVISORY : IVANTI SENTRY CRITICAL RCE & AUTHENTICATION BYPASS - CVE-2026-10520 / CVE-2026-10523

- **Cyber Centre Recommendation:** Immediately upgrade all Ivanti Sentry appliances to fixed versions 10.5.2, 10.6.2, or 10.7.1 and treat exposed Sentry gateways as high-risk assets requiring compromise review before restoration.
- **Broad Threat Coverage:**
 - CVE-2026-10520 is a CVSS 10.0 OS command-injection flaw allowing unauthenticated remote attackers to achieve root-level remote code execution.
 - CVE-2026-10523 is a CVSS 9.9 authentication-bypass flaw allowing unauthenticated attackers to create arbitrary admin accounts and gain full administrative access.
- **Proactive Cybersecurity Measure:**
 - Patch immediately and restrict Sentry administrative access to trusted management networks only.
 - Review Sentry logs for suspicious admin-account creation, command execution, configuration changes, and unknown external access.
 - Rotate credentials/tokens associated with mobile device management, email gateways, and backend enterprise integrations.
 - Restrict cPanel/WHM access to trusted IPs and disable public exposure where not operationally required.

Read more at: Security Advisory Ivanti Sentry (CVE-2026-10520, CVE-2026-10523)

ADVISORY : GOOGLE CHROME / CHROMIUM V8 ZERO-DAY EXPLOITED IN THE WILD - CVE-2026-11645

- **Cyber Centre Recommendation:** Push emergency updates for Google Chrome and all Chromium-based browsers across managed endpoints; prioritize high-risk user groups, VDI environments, and unmanaged/BYOD devices accessing corporate applications. Google released fixes in June 2026 and acknowledged active exploitation in the wild.
- **Broad Threat Coverage:**
 - CVE-2026-11645 is a high-severity out-of-bounds read/write flaw in V8, Chrome's JavaScript and WebAssembly engine.
 - Exploitation can allow a remote attacker to execute arbitrary code inside the browser sandbox via a crafted HTML page..
- **Proactive Cybersecurity Measure:**
 - Update Chrome to 149.0.7827.102/103 or later and validate browser-version compliance through endpoint management tools.
 - Apply parallel updates for Chromium-based browsers such as Microsoft Edge, Brave, Opera, and Vivaldi as vendor patches become available.
 - Monitor endpoint telemetry for abnormal browser child processes, suspicious script execution, and unexpected network connections after browser activity.

Read more at: Google Chrome V8 Zero-Day Coverage