iSec Security Consulting
Information Security & Compliance

iChek Services
Background Verification & HR Risk

🔐 THE iSEC & iCHEK MONTHLY BRIEF · October 2026 Edition

67.6M Records Breached. 86% of Firms Hit by Hiring Fraud. October 2026's Twin Crisis for Every Risk Leader.

> Oracle Health's 20-million-patient exposure, a record 1,413-CVE Patch Tuesday, Checkr's finding that 86% of organisations experienced hiring fraud this year, and 38% suspect a fraudster is already on their payroll — October 2026 makes the case that cybersecurity and workforce integrity are now the same risk conversation. This edition covers both.

🔐 iSec Threat Intelligence — October 2026

Global & India cybersecurity incidents, vulnerabilities, and regulatory developments

67.6M
Records breached globally in October 2026 across 49 confirmed incidents (GRC Solutions)

1,413
CVEs patched in Microsoft's October Patch Tuesday — a record single-month volume

20M
Patient records exposed in Oracle Health (Cerner) breach — traced to 2025 credential abuse

🌐 Global Threat Watch

MAJOR BREACH

Oracle Health (Cerner): 20 million patient records exposed — traced to 2025 credential abuse

State attorney-general filings confirmed approximately 20 million patient records compromised via attacker use of stolen customer credentials against legacy Cerner systems — access that persisted undetected from 2025 into 2026. A defining case for the dangers of long-unrotated credentials, legacy EHR infrastructure, and absent anomaly detection. Every organisation using Oracle Health or legacy EHR platforms must urgently audit credential hygiene and legacy system access controls.

AI SUPPLY CHAIN

Malicious LiteLLM 1.107.0 published to PyPI and official Docker images — credential stealer in production

Attackers abused compromised GitHub tokens to publish a malicious LiteLLM release carrying a credential stealer and backdoor. Available for approximately two hours via official channels before removal. Root cause: an internal key exposed in May was never revoked. The second LiteLLM security incident of 2026, confirming that AI toolchain supply chain security requires the same rigour as production application dependencies.

CRITICAL CVE

PHP core RCE (CVE-2026-109618 & 109619, CVSS 9.2) — exploited in the wild after details leaked

Two unauthenticated RCE flaws in PHP core were emergency-patched on October 21 after technical details leaked ahead of scheduled disclosure. Exploitation in the wild reported within hours. PHP powers approximately 77% of server-side web applications globally. Organisations must verify patch status across all PHP-based applications and enforce WAF rules blocking exploitation attempts.

RECORD PATCH DAY

Microsoft October Patch Tuesday: record 1,413 CVEs including Windows Shell zero-day in active exploitation

A record single-cycle release including CVE-2026-96951, a Windows Shell security-feature bypass confirmed as actively exploited before patching. The volume underscores the industrialisation of vulnerability research and makes manual patch prioritisation operationally impossible at enterprise scale. Automated, risk-based patch management is now a baseline operational requirement.

🇮🇳 India Threat Radar

INDIA ALERT

SBI customer records appear on dark web — 375,000 records including PII under investigation

A dark-web dataset containing approximately 375,000 SBI customer records surfaced in October 2026, of which 3,897 contained personally identifiable information. The source remains under investigation — a direct breach of SBI's core systems has not been confirmed. The incident highlights the persistent risk from third-party data aggregators, fintech partners, and API integrations holding banking customer data with weaker security controls than the primary institution.

CERTIFICATE CRISIS

eMudhra intermediate CA certificates revoked globally — weak private keys found in public certs

India-based CA eMudhra faced a global revocation event when researchers found private keys for eight intermediate CAs could be recovered directly from public certificates due to weak key generation. Major browsers and vendors revoked the affected intermediates. The incident raises serious questions about PKI governance at Indian certificate authorities — particularly those issuing certificates for critical government and banking infrastructure.

CERT-IN

CERT-In urges 12-hour patch cycles as AI compresses zero-day exploitation windows

CERT-In's October advisory calls for 12-hour patch cycles where feasible, as AI-driven exploitation is compressing the window between vulnerability disclosure and active attack from days to hours. Microsoft Windows, Office, and cloud authentication vulnerabilities are flagged as the highest-priority patching surface. The 6-hour breach notification requirement for personal data incidents remains non-negotiable.

⚡ iSec Advisory: Non-Human Identities Are Your Invisible Attack Surface

The ConnectWise compromise, the LiteLLM supply chain attack, and the Oracle Health credential breach share one vector: application tokens, service accounts, and API keys with excessive permissions and no rotation policy. These non-human identities outnumber human

users by an order of magnitude, are rarely covered by MFA, and are systematically excluded from identity governance programmes. iSec's Zero Trust Architecture and VAPT services now include dedicated non-human identity assessment — because the breach your EDR won't catch may already be in your secrets manager.

ISEC PRODUCT — NOW LIVE

VulnScanAI — All Your Security Tools. One AI-Powered Platform.

Nmap, OWASP ZAP, and leading VAPT tools unified. Every finding re-analysed by AI. PII automatically masked. DPDP, RBI & SEBI compliance built in.

Unified Scanning Engine

All tools, one dashboard — no siloed findings, no context switching

AI Re-Analysis

Every vulnerability contextualised, prioritised & turned into remediation steps

Automatic PII Masking

Personal data masked in reports by default — share safely

Windows / Linux / Mac Agents

Lightweight cross-platform agents for full estate coverage

DPDP Act | RBI Security Audit | SEBI Mandated Assessments | ISO 27001 | CERT-In Compliance

Free version available — try the full platform with no commitment at isecai.io

Try VulnScanAI Free → isecai.io

VAPT — Web, Mobile & Network

Vulnerability assessment & penetration testing

ISO 27001 / ISMS Consulting

Certification-ready implementation & gap audits

CERT-In & DPDP Compliance

6-hour reporting readiness & data protection

Zero Trust Architecture

Identity, access governance & network segmentation

Incident Response & Forensics

Rapid containment, investigation & recovery

Security Awareness Training

Phishing simulations & workforce upskilling

🌻 iChek Hiring Intelligence — October 2026

Global & India background verification, HR risk, and workforce compliance intelligence

86%
of organisations experienced hiring fraud in the past year — Checkr Hiring Hoax Survey 2026

42%
of fraudulent candidates pass pre-hire screening and start the job — HYPR 2026

58%
of managers believe an employee may hold another job simultaneously — Checkr 2026

🌐 Global Hiring Risk Watch

AI FRAUD

Checkr 2026 (3,000 US managers): 40% interviewed a fake-identity candidate — up from 31% last year

86% of organisations experienced at least one type of hiring fraud in the past year. 40% interviewed a candidate later found to be using a fake identity. Most strikingly, 38% suspect a fraudulent employee is on their payroll right now, with an average of 5.73 days of unmonitored system access before detection. 28% admitted advancing a candidate they suspected of dishonesty because the role needed filling urgently.

DEEPFAKE DETECTION

Pin 2026: 22% of recruiters confirmed a deepfake in a video interview — human detection near chance

22.4% of 475+ recruiters confirmed a deepfake or identity swap in a video interview; 16.3% more suspected one but could not prove it. Human deepfake detection accuracy in a large-scale meta-analysis: 55.54% — barely above a coin flip. 68% of hiring managers say candidates are now better at faking identities with AI than employers are at catching them.

POST-HIRE RISK

HYPR 2026: 98% experienced candidate fraud — 44% have no post-hire identity verification process

HYPR's State of HR Identity Fraud Detection report finds near-universal exposure: 98% experienced candidate fraud firsthand. For 42%, the fraud was discovered only after the hire was made. For one in four companies, resolution took one to three months. Despite this, 44% have no formal post-hire identity verification process — leaving the largest gap wide open.

🇮🇳 India Hiring Intelligence

DPDP DEADLINE

DPDP Act consent manager framework activates November 2026 — BGV programmes must be ready now

India's DPDP Rules consent manager framework activates in November 2026, requiring all BGV programmes to demonstrate that candidate consent was collected digitally, covers only the specific checks conducted, and that data handling is fully auditable. Organisations running manual or email-based BGV workflows will find themselves non-compliant. Full rights obligations — notice, security, breach reporting — follow on 13 May 2027.

ICHEK INTELLIGENCE

iChek verification data: post-hire fraud emerging as India's fastest-growing BGV blind spot

iChek's October 2026 verification intelligence identifies a widening gap in Indian enterprise hiring: while pre-hire checks are increasingly standard, the post-hire period remains largely unmonitored. Duplicate employment via UAN manipulation, qualification upgrades on internal HR records, and undisclosed concurrent roles are the fastest-growing fraud patterns among India's mid-to-senior workforce — and are systematically missed by one-time pre-employment checks.

SECTOR ALERT

Healthcare and pharma BGV: highest-stakes sector sees rising credential fraud in India

India's healthcare and pharmaceutical sectors present a uniquely elevated BGV risk profile. Fabricated nursing, pharmacy, and clinical research credentials are increasing across private hospital groups and pharmaceutical manufacturers — where a fraudulent qualification is not merely a contractual issue but a potential patient safety incident. Mid-career lateral hires represent the highest-risk cohort.

📌 iChek Insight: The 5.73-Day Window Is Your Biggest Risk

HYPR's data is stark: when a fraudulent candidate makes it past pre-hire screening, they average 5.73 days of unmonitored access before detection. In that window, they can exfiltrate data, establish persistence, or cause damage that takes months and six-figure sums to remediate. iChek's continuous post-hire monitoring — combining periodic re-verification, UAN dual employment audits, behavioural risk flags, and social media risk mapping — closes the gap that one-time pre-hire checks leave wide open.

Pre-Employment Screening

Identity, education, employment & criminal verification

Continuous Monitoring

Ongoing post-hire risk tracking & re-verification

Moonlighting Detection

UAN & EPFO cross-checks for dual employment

Drug & Alcohol Testing

Certified testing for safety-critical roles

Social Media Risk Mapping

Conduct & reputational risk profiling

International Verification

Seamless screening across 150+ countries

Secure Your Organisation with iSec

Expert information security consulting across India and beyond.

contactus@isec.co.in

www.isec.co.in

Secure Your Next Hire with iChek

15 years securing India's finest workforces.

info@ichek.info

www.ichek.info