**iSec Security Consulting**
Information Security & Compliance

**iChek Services**
Background Verification & HR Risk

THE iSEC & iCHEK MONTHLY BRIEF · October 2026 Edition

# 86% of Firms Hit by Hiring Fraud, 67.6M Records Breached: October 2026's Twin Crisis

> Oracle Health's reported 20-million-record exposure, a record Microsoft Patch Tuesday of more than 1,400 CVEs, Checkr's finding that 86% of organisations experienced hiring fraud this year, and 38% of managers suspecting a fraudulent employee is already on their payroll: October 2026 shows that cybersecurity and workforce integrity are one risk conversation. This edition covers both. Every figure names its source.

## iSec Threat Intelligence — October 2026

Global & India cybersecurity incidents, vulnerabilities and regulatory developments

**67.6M**
confirmed records breached in October 2026, a floor counted across 17 of the 49 incidents GRC Solutions tracked

**1,400+**
CVEs in Microsoft's October Patch Tuesday, a record (trackers count 1,411 to 1,415), with three zero-days

**~20M**
patient records reported exposed in the Oracle Health (Cerner) breach (Texas Attorney General filing)

## Global Threat Watch

MAJOR BREACH

### Oracle Health (Cerner): about 20 million patient records reported exposed

A Texas Attorney General filing reported that roughly 20 million patient records were affected in the Oracle Health (Cerner) data breach. How the attackers got in has not been confirmed in the sources

we could verify, so treat any root-cause claim with caution. Organisations on Oracle Health or legacy health-record platforms should review credential hygiene and legacy-system access.

Source: Texas Attorney General filing, as reported by SecurityWeek, Oct 2026.

AI SUPPLY CHAIN

### Malicious LiteLLM 1.107.0 published to PyPI and official Docker images, carrying a credential stealer

LiteLLM said the malicious release was published through three engineers' GitHub accounts, apparently using stolen GitHub CLI OAuth tokens. The package carried a credential stealer and a backdoor, and the PyPI package and Docker images were pulled. LiteLLM had not established how the tokens were obtained. It is at least the second LiteLLM compromise of 2026, and it shows that AI toolchains need the same supply-chain rigour as production dependencies.

Source: The Hacker News, Oct 2026.

CRITICAL CVE

### PHP core remote-code-execution flaws (CVE-2026-109618 & CVE-2026-109619) emergency-patched

The PHP project shipped emergency patches for two critical remote-code-execution flaws, reportedly after details leaked ahead of scheduled disclosure. Check the PHP version on every application you run, apply the patched release, and use WAF rules as a stop-gap.

Source: BleepingComputer; Health-ISAC bulletin, 21 Oct 2026.

RECORD PATCH DAY

### Microsoft October Patch Tuesday: a record release of about 1,400 CVEs, with three zero-days

Trackers count 1,411 to 1,415 CVEs and three zero-days, one of them a Windows Shell flaw reported as exploited before the patch. Volume like this makes manual patch prioritisation unworkable at enterprise scale, so risk-based patch management is now a baseline.

Source: BleepingComputer (1,411); other trackers report up to 1,415.

## India Threat Radar

INDIA ALERT

### SBI confirms 3,897 customer records in a roughly 375,000-record dark-web dump

In an October 21 stock-exchange filing, SBI said 3,897 of its customer records appear in a dark-web dataset of roughly 375,000 rows posted by a threat actor. The source of the data is not yet known, and SBI said account balances and funds are safe. The remaining records have not been tied to SBI. It is a reminder to check what customer data sits with partners and aggregators.

Source: DT Next, Oct 2026. Origin unconfirmed.

CERTIFICATE CRISIS

### eMudhra intermediate CA certificates blocked after weak private keys found

The private keys of eight eMudhra intermediate CAs (six for TLS, two for code signing) were recoverable from their public certificates because of weak randomness in key generation. Google, Mozilla and Cloudflare blocked them. eMudhra said none of the eight had issued end-entity certificates. Organisations should confirm their trust stores have the updates.

Source: CSO Online, Oct 2026.

CERT-IN

### CERT-In guidance sets a 12-hour patch target for exploited, internet-facing flaws

CERT-In's guidance, published in May 2026, recommends patching known-exploited vulnerabilities on internet-facing systems within 12 hours where feasible, other critical exposed flaws within a day, and high-severity ones within five days, citing AI-assisted exploitation. Separately, the existing requirement to report cyber incidents to CERT-In within 6 hours still applies.

Source: The Hacker News, 26 May 2026. The binding force of the 12-hour target is unclear.

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

The ConnectWise Cloud Backup compromise (a stolen application credential used to reach at least 162 Microsoft 365 tenants, per Huntress) and the LiteLLM attack (stolen developer OAuth tokens) both turned on credentials held by software and not by people. Service accounts, application tokens and API keys are often over-permissioned, unrotated and outside MFA and identity governance. Rotate and scope every token and service account, and treat the secrets manager as part of your attack surface.

ISEC PRODUCT

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

Nmap, OWASP ZAP and leading VAPT tools in one platform. Findings re-analysed by AI. PII masked in reports.

**Unified Scanning Engine**

All tools, one dashboard

**AI Re-Analysis**

Findings contextualised and prioritised, with remediation steps

**Automatic PII Masking**

Personal data masked in reports

**Windows / Linux / Mac Agents**

Cross-platform agents

Free version available at isecai.io

**Try VulnScanAI Free → isecai.io**

**VAPT — Web, Mobile & Network**

Vulnerability assessment & penetration testing

**ISO 27001 / ISMS Consulting**

Implementation & gap audits

**CERT-In & DPDP Compliance**

Incident-reporting readiness & data protection

**Zero Trust Architecture**

Identity, access governance & segmentation

**Incident Response & Forensics**

Containment, investigation & recovery

**Security Awareness Training**

Phishing simulations & workforce upskilling

## iChek Hiring Intelligence — October 2026

Global & India background verification, HR risk and workforce compliance

**86%**

of organisations experienced hiring fraud in the past year — Checkr Hiring Hoax 2026 (3,000 US managers)

**42%**

of identified candidate-fraud cases escaped pre-hire detection — 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. 38% suspect a fraudulent employee is on their payroll right now. 28% admitted advancing a candidate they suspected of dishonesty because the role needed filling urgently.

Source: Checkr, Hiring Hoax 2026, online survey, 11–16 Sep 2026. Self-reported, US only.

DEEPFAKE DETECTION

### Pin 2026: 22% of surveyed recruiters confirmed a deepfake in a video interview

In a survey of recruiters using Pin's platform, 22.4% said they had confirmed a deepfake or identity swap in a video interview, and 16.3% more suspected one but could not prove it. It is a vendor survey of its own users, not a measure of all hiring.

Source: Pin, 2026 deepfake candidate report.

POST-HIRE RISK

### HYPR 2026: 98% of HR leaders have faced candidate fraud, and 42% of cases slip past pre-hire checks

HYPR's State of HR Identity Fraud Detection report finds near-universal exposure: 98% of HR leaders have experienced candidate fraud firsthand, and in 42% of cases the fraud escaped pre-hire detection. Once it escaped, detection was slow: fewer than 3% were flagged the same day, 45% took four to six days, and about one in five went undetected for up to three weeks.

Source: HYPR, reported by Biometric Update, Sep 2026.

## India Hiring Intelligence

DPDP TIMELINE

### DPDP consent managers go live in November 2026; the main duties follow on 13 May 2027

The consent-manager provisions of the DPDP Rules take effect in November 2026. Consent managers are an option for candidates and not a requirement for employers, but they will change how consent is given and withdrawn, so background-verification programmes should be ready to record that consent was collected digitally, covers only the checks actually run, and can be audited. Notice, security and breach-reporting duties for data fiduciaries begin on 13 May 2027.

Source: DPDP Rules 2025 commencement schedule; commentary by Ampcus Cyber.

SECTOR ALERT

### Healthcare and pharma: fake-degree cases keep surfacing in the highest-stakes sector

Indian police have recently busted rackets issuing fake pharmacy (B.Pharma) and medical (MBBS) credentials. Where a false qualification is a potential patient-safety incident and not only a contract issue, hospitals and pharma employers should verify degrees and registrations directly with the issuing university or council, including for lateral hires.

Source: news reports in Medical Dialogues. Individual cases; no trend rate is claimed.

### iChek Insight: The Window After the Hire Is Your Biggest Risk

When a fraudulent candidate gets past pre-hire screening, the damage happens before anyone notices. In HYPR's data, 45% of such cases took four to six days to detect and about one in five took up to three weeks. In that window a person can copy data, set up persistence, or cause damage that takes months to repair. Continuous post-hire monitoring (periodic re-verification, UAN dual-employment audits, behavioural risk flags and social-media risk mapping) closes the gap that a one-time check leaves.

**Pre-Employment Screening**

Identity, education, employment & criminal verification

**Continuous Monitoring**

Post-hire 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**

Screening outside India


### Secure Your Organisation with iSec

Information security consulting since 2001.

contactus@isec.co.in

www.isec.co.in

### Secure Your Next Hire with iChek

15+ years in pre-employment background screening.

info@ichek.info

www.ichek.info

Notes: Published 7 November 2026. Survey figures are self-reported and describe the respondents, not all hiring. Incident details were still developing at the time of writing; figures can change as investigations conclude.