Nucleus Systems

SWIPE →

CODE TRUST ASSURANCE · NUCLEUS SYSTEMS

BLACK OCTOBER

21 verified incidents · October 2026

The software supply chain's worst month on record. Every entry is dated to when the incident happened, not when it surfaced — and separated by what it actually establishes.

- 8 supply chain compromises
- 8 platform and data breaches
- 5 vulnerability disclosures

codetrustassurance.com

CONTINUES →

HOW TO READ THIS

An advisory is not a breach. A signature is not safety.

01

Supply chain compromise

Malicious code reached users through a channel they already trusted — a package registry, an update server, a signed release. The distribution mechanism worked exactly as designed.

02

Platform or data breach

Unauthorised access confirmed by the affected organisation itself. Records, credentials or customer secrets were reached.

03

Vulnerability disclosure

A flaw was published. On its own that establishes neither exploitation nor a breach — though two of the five here were attacked before a fix existed.

CONTINUES →

SUPPLY CHAIN · 1 OF 3

Malicious code, through a trusted channel

Eight releases reached users carrying code the maintainers never wrote.

Oct 5

SubQuery npm package backdoored

@subql/common 5.8.3 — the publish workflow swapped the local build for an external archive before trusted publishing.

Vendor advisory · supply-chain research

Oct 7+

GhostAction targets GitHub repositories

Stolen personal access tokens pushed malicious workflows across repositories, harvesting package, cloud and AI credentials.

Supply-chain research

Oct 8

Tensorlake publishes a malicious npm package

0.5.144 — a rogue commit published through the release workflow, carrying a dead-man's switch.

Supply-chain research

CONTINUES →

SUPPLY CHAIN · 2 OF 3

The channel authenticated. The contents did not.

In each case the publishing mechanism worked correctly.

Oct 15–16

Rank Math PRO update delivers malware

3.0.123 — the update channel served backdoored files for eleven hours, installing a self-restoring backdoor.

WordPress security research

Oct 17

eMudhra certificate authority keys compromised

Eight intermediate CA private keys generated with insufficient entropy and recoverable — enough to forge TLS certificates.

eMudhra statements

Oct 17–18

UpdraftPlus customer data compromised

Stolen keys were used to push backdoored plugins through UpdraftCentral to customer sites.

UpdraftPlus security report

CONTINUES →

SUPPLY CHAIN · 3 OF 3

Two that reached the widest audience

A cloud CLI and a package pulled millions of times a day.

Oct 19

OVHcloud CLI binaries backdoored

v0.11.0–v0.15.0 — a contributor account hijack replaced release assets and their checksums for 94 minutes.

OVHcloud security advisory

Oct 21

LiteLLM ships a malicious release

1.107.0 — all seven PyPI wheels and the Docker images carried a credential stealer and a remote loader.

LiteLLM advisory · Datadog Security Labs

CONTINUES →

BREACH · 1 OF 3

Unauthorised access, confirmed

Each disclosed by the organisation it happened to.

Oct 7

IDCF Cloud hit by ransomware

495 organisations affected across Japan. Four zones were left unrecoverable and backups failed.

IDC Frontier · BleepingComputer

Oct 7

Nikkei reports 1.83M records exposed

A cloud service used for system development was accessed. Disclosed on 16 October.

Nikkei Inc. · Personal Information Protection Commission

Oct 13–17

ConnectWise cloud backup identities compromised

A stolen application credential signed into between 162 and 173 Microsoft 365 tenants.

ConnectWise threat brief

CONTINUES →

BREACH · 2 OF 3

Credentials were the way in — and across

Long-lived keys turned single incidents into platform-wide ones.

Oct 14–15

Zeabur infrastructure breached

321,810 accounts and 3.2 million environment-variable records. The second breach in two months.

Zeabur post-mortem

Oct 16

OpenCode Console exposes AI API keys

1.4% of Console users affected, with provider API keys among the exposed material.

OpenCode disclosure

Oct 19

Capcom reports unauthorised access

11,774,247 records — email addresses and login metadata.

Capcom Co., Ltd. · regulatory filings

CONTINUES →

BREACH · 3 OF 3

Access that went unnoticed for weeks

Duration matters as much as scope.

Oct 19

TiDB Cloud breach disclosed

Stolen service account credentials gave 48 days of access, from 9 September to 7 October.

PingCAP disclosure

Oct 21

Railway customer secrets exposed

Environment variables were accessed and some decrypted. Railway states the aim was AI inference keys.

Railway incident report

CONTINUES →

VULNERABILITY · 1 OF 2

Published flaws, two already exploited

Severity is the vendor's own rating, not an estimate.

Oct 12+

GitLab — CVSS 10.0

CVE-2026-97229. An integer overflow allowing unauthenticated remote code execution on self-managed instances.

GitLab security release

Oct 20–21

PHP2Shell — exploited before the fix

CVE-2026-109618 and 109619. Interpreter flaws leaked a day early and attacked before patches shipped.

PHP Group · CISA KEV

Oct 21

Node.js patches ten CVEs

Including a Brotli remote code execution flaw and TLS hostname verification bypasses.

Node.js Foundation

CONTINUES →

VULNERABILITY · 2 OF 2

The infrastructure everything else sits on

The kernel and the DNS server beneath most of the internet.

Oct 22

Linux kernel — CVSS 9.8

CVE-2026-98432. A TCP stack flaw affecting Ubuntu, Red Hat Enterprise Linux and other distributions.

Linux kernel CVE team

Oct 30

BIND 9.18 — multiple CVEs

Several vulnerabilities addressed across vendor advisories for the most widely deployed DNS server.

ISC · vendor advisories

CONTINUES →

THE PATTERN UNDERNEATH

Three failures, repeating

01

A signature says who signed, not whether they were compromised

LiteLLM's malicious release was signed and published through the genuine pipeline, after an organisation owner's token overrode branch protection.

02

Encryption at rest fails when one identity can both read and decrypt

Railway's stored environment variables were encrypted. Some were still obtained in plaintext through compromised internal systems.

03

Unrotated credentials turn one incident into the next

Zeabur's second breach used an admin token and AWS keys never rotated after the first, two months earlier.

CONTINUES →

If an attacker had one of your credentials today, what would stop them?

Not what your policy says — what your controls demonstrably refuse to do, tested, with evidence a third party can check.

86	controls across six weighted domains
5	scoring axes, against a five-level maturity scale
CTA-1–4	certification, listed in a public Trust Registry

Full analysis and every source: codetrustassurance.com/insights