CYBER NEWSLETTER

Saturday, Jan 17, 2026 • 06:33 UTC

THREAT PULSE

Zero-Days 5
Ransomware 0
Breaches 2
Phishing 0
Other 3

TOP 10

1. China-Linked APT Exploited Sitecore Zero-Day in Critical Infrastructure Intrusions
2. Cisco Patches Zero-Day RCE Exploited by China-Linked APT in Secure Email Gateways
3. Critical WordPress Modular DS Plugin Flaw Actively Exploited to Gain Admin Access
4. Cisco finally patches seven-week-old zero-day flaw in Secure Email Gateway products
5. Microsoft Fixes 114 Windows Flaws in January 2026 Patch, One Actively Exploited
6. Critical flaw in AWS Console risked compromise of build environment
7. 750,000 Impacted by Data Breach at Canadian Investment Watchdog
8. AWS CodeBuild Misconfiguration Exposed GitHub Repos to Potential Supply Chain Attacks
9. Fortinet Fixes Critical FortiSIEM Flaw Allowing Unauthenticated Remote Code
10. New Vulnerability in n8n

Lookback: 72h • Ranked by risk

ZERO-DAYS

China-Linked APT Exploited Sitecore Zero-Day in Critical Infrastructure Intrusions

The Hacker News • ■■■■ 128.1 • 23.3h
A threat actor likely aligned with China has been observed targeting critical infrastructure sectors in North America since at least last year. Cisco Talos, which is tracking the
Why it matters: zero-day, apt.
https://thehackernews.com/2026/01/china-linked-apt-exploits-sitecore-zero.html

Cisco finally patches seven-week-old zero-day flaw in Secure Email Gateway products

CSO Online • ■■■■ 119.0 • 11.7h
Better late than never. Cisco this week patched a ‘critical’ zero-day flaw in the company’s email security and management gateways that has hung over customers’
Why it matters: zero-day, critical.
https://www.csoonline.com/article/4118159/cisco-finally-patches-seven-week-old-zero-day-flaw-in-secure-email-gateway-products-2.html

Microsoft Fixes 114 Windows Flaws in January 2026 Patch, One Actively Exploited

The Hacker News • ■■■■ 116.3 • 68.9h
Microsoft on Tuesday rolled out its first security update for 2026, addressing 114 security flaws, including one vulnerability that it said has been actively exploited in the
Why it matters: actively exploited, in the wild.
https://thehackernews.com/2026/01/microsoft-fixes-114-windows-flaws-in.html

OTHER

Cisco Patches Zero-Day RCE Exploited by China-Linked APT in Secure Email Gateways

The Hacker News • ■■■■ 128.0 • 24.9h
Cisco on Thursday released security updates for a maximum-severity security flaw impacting Cisco AsyncOS Software for Cisco Secure Email Gateway and
Why it matters: zero-day, apt.
https://thehackernews.com/2026/01/cisco-patches-zero-day-rce-exploited-by.html

Critical WordPress Modular DS Plugin Flaw Actively Exploited to Gain Admin Access

The Hacker News • ■■■■ 125.9 • 39.0h
A maximum-severity security flaw in a WordPress plugin called Modular DS has come under active exploitation in the wild, according to Patchstack. The vulnerability,
Why it matters: actively exploited, in the wild.
https://thehackernews.com/2026/01/critical-wordpress-modular-ds-plugin.html

BREACHES

Critical flaw in AWS Console risked compromise of build environment

Cybersecurity Dive • ■■■■ 109.9 • 38.6h
The CodeBreach vulnerability could have enabled a massive supply chain attack, researchers warn.
Why it matters: breach, critical.
https://www.cybersecuritydive.com/news/critical-flaw-in-aws-console-risked-compromise-of-build-environment/809745/

750,000 Impacted by Data Breach at Canadian Investment Watchdog

SecurityWeek • ■■■■ 98.6 • 18.0h
The incident impacted the personal information of CIRO member firms and their registered employees. The post 750,000 Impacted by Data Breach at Canadian Investment
Why it matters: data breach, breach.
https://www.securityweek.com/750000-impacted-by-data-breach-at-canadian-investment-watchdog/

CYBER NEWSLETTER

Saturday, Jan 17, 2026 • 06:33 UTC

THREAT PULSE

Zero-Days 5
Ransomware 0
Breaches 2
Phishing 0
Other 3

TOP 10

Lookback: 72h • Ranked by risk

AWS CodeBuild Misconfiguration Exposed GitHub Repos to Potential Supply Chain

The Hacker News • ■■■■ 96.6 • 35.0h
A critical misconfiguration in Amazon Web Services (AWS) CodeBuild could have allowed complete takeover of the cloud service provider's own GitHub repositories,
Why it matters: critical, supply chain.
https://thehackernews.com/2026/01/aws-codebuild-misconfiguration-exposed.html

Fortinet Fixes Critical FortiSIEM Flaw Allowing Unauthenticated Remote Code

The Hacker News • ■■■■ 92.2 • 66.7h
Fortinet has released updates to fix a critical security flaw impacting FortiSIEM that could allow an unauthenticated attacker to achieve code execution on susceptible
Why it matters: critical, remote code execution.
https://thehackernews.com/2026/01/fortinet-fixes-critical-fortisiem-flaw.html

New Vulnerability in n8n

Schneier on Security • ■■■■ 80.1 • 42.5h
This isn’t good: We discovered a critical vulnerability (CVE-2026-21858, CVSS 10.0) in n8n that enables attackers to take over locally deployed instances,
Why it matters: critical, cve.
https://www.schneier.com/blog/archives/2026/01/new-vulnerability-in-n8n.html