CYBER NEWSLETTER

Sunday, Jan 18, 2026 • 17:52 UTC

THREAT PULSE

Zero-Days 3
Ransomware 1
Breaches 1
Phishing 1
Other 4

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. Cisco finally patches seven-week-old zero-day flaw in Secure Email Gateway products
4. 750,000 Impacted by Data Breach at Canadian Investment Watchdog
5. AWS CodeBuild Misconfiguration Exposed GitHub Repos to Potential Supply Chain Attacks
6. Black Basta Ransomware Leader Added to EU Most Wanted and INTERPOL Red Notice
7. More Problems for Fortinet: Critical FortiSIEM Flaw Exploited
8. LOTUSLITE Backdoor Targets U.S. Policy Entities Using Venezuela-Themed Spear Phishing
9. GootLoader Malware Uses 500–1,000 Concatenated ZIP Archives to Evade Detection
10. WhisperPair Attack Leaves Millions of Audio Accessories Open to Hijacking

Lookback: 72h • Ranked by risk

ZERO-DAYS

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

The Hacker News • ■■■■ 120.3 • 58.6h
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

RANSOMWARE

Black Basta Ransomware Leader Added to EU Most Wanted and INTERPOL Red Notice

The Hacker News • ■■■■ 82.9 • 25.4h
Ukrainian and German law enforcement authorities have identified two Ukrainians suspected of working for the Russia-linked ransomware-as-a-service (RaaS) group
Why it matters: ransomware, trusted source.
https://thehackernews.com/2026/01/black-basta-ransomware-hacker-leader.html

BREACHES

750,000 Impacted by Data Breach at Canadian Investment Watchdog

SecurityWeek • ■■■■ 92.2 • 53.3h
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/

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

The Hacker News • ■■■■ 119.7 • 60.2h
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

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

CSO Online • ■■■■ 114.0 • 47.0h
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

PHISHING

LOTUSLITE Backdoor Targets U.S. Policy Entities Using Venezuela-Themed Spear

The Hacker News • ■■■■ 71.5 • 55.4h
Security experts have disclosed details of a new campaign that has targeted U.S. government and policy entities using politically themed lures to deliver a backdoor known as
Why it matters: malware, phishing.
https://thehackernews.com/2026/01/lotuslite-backdoor-targets-us-policy.html

OTHER

CYBER NEWSLETTER

Sunday, Jan 18, 2026 • 17:52 UTC

THREAT PULSE

Zero-Days 3
Ransomware 1
Breaches 1
Phishing 1
Other 4

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. Cisco finally patches seven-week-old zero-day flaw in Secure Email Gateway products
4. 750,000 Impacted by Data Breach at Canadian Investment Watchdog
5. AWS CodeBuild Misconfiguration Exposed GitHub Repos to Potential Supply Chain Attacks
6. Black Basta Ransomware Leader Added to EU Most Wanted and INTERPOL Red Notice
7. More Problems for Fortinet: Critical FortiSIEM Flaw Exploited
8. LOTUSLITE Backdoor Targets U.S. Policy Entities Using Venezuela-Themed Spear Phishing
9. GootLoader Malware Uses 500–1,000 Concatenated ZIP Archives to Evade Detection
10. WhisperPair Attack Leaves Millions of Audio Accessories Open to Hijacking

Lookback: 72h • Ranked by risk

AWS CodeBuild Misconfiguration Exposed GitHub Repos to Potential Supply Chain

The Hacker News • ■■■■ 85.7 • 70.4h
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

More Problems for Fortinet: Critical FortiSIEM Flaw Exploited

Dark Reading • ■■■■ 74.6 • 44.8h
CVE-2025-64155, a command injection vulnerability, was disclosed earlier this week and quickly came under attack from a variety of IP addresses.
Why it matters: critical, cve.
https://www.darkreading.com/vulnerabilities-threats/fortinet-critical-fortisiem-flaw-exploited

WhisperPair Attack Leaves Millions of Audio Accessories Open to Hijacking

SecurityWeek • ■■■■ 61.9 • 54.0h
The critical issue impacts Bluetooth audio accessories with improper Google Fast Pair implementations. The post WhisperPair Attack Leaves Millions of Audio Accessories
Why it matters: critical, trusted source.
https://www.securityweek.com/whisperpair-attack-leaves-millions-of-bluetooth-accessories-open-to-hijacking/

GootLoader Malware Uses 500–1,000 Concatenated ZIP Archives to Evade Detection

The Hacker News • ■■■■ 63.8 • 47.9h
The JavaScript (aka JScript) malware loader called GootLoader has been observed using a malformed ZIP archive that's designed to sidestep detection efforts by
Why it matters: malware, trusted source.
https://thehackernews.com/2026/01/gootloader-malware-uses-5001000.html