CYBER NEWSLETTER

Friday, Jan 16, 2026 • 07:23 UTC

THREAT PULSE

Zero-Days 3
Ransomware 0
Breaches 3
Phishing 0
Other 4

TOP 10

1. Cisco Patches Zero-Day RCE Exploited by China-Linked APT in Secure Email Gateways
2. Critical WordPress Modular DS Plugin Flaw Actively Exploited to Gain Admin Access
3. Microsoft Fixes 114 Windows Flaws in January 2026 Patch, One Actively Exploited
4. Critical flaw in AWS Console risked compromise of build environment
5. Fortinet Fixes Critical FortiSIEM Flaw Allowing Unauthenticated Remote Code
6. AWS CodeBuild Misconfiguration Exposed GitHub Repos to Potential Supply Chain Attacks
7. Central Maine Healthcare Data Breach Impacts 145,000 Individuals
8. Traveler Information Stolen in Eurail Data Breach
9. New ‘StackWarp’ Attack Threatens Confidential VMs on AMD Processors
10. New Vulnerability in n8n

Lookback: 72h • Ranked by risk

ZERO-DAYS

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

The Hacker News • ■■■■ 129.4 • 1.8h
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

BREACHES

Critical flaw in AWS Console risked compromise of build environment

Cybersecurity Dive • ■■■■ 112.8 • 15.5h
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/

Central Maine Healthcare Data Breach Impacts 145,000 Individuals

SecurityWeek • ■■■■ 98.4 • 20.8h
Hackers stole patients’ personal, treatment, and health insurance information from the organization’s IT systems. The post Central Maine Healthcare Data Breach Impacts
Why it matters: data breach, breach.
https://www.securityweek.com/central-maine-healthcare-data-breach-impacts-145000-individuals/

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

The Hacker News • ■■■■ 128.7 • 15.9h
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

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

The Hacker News • ■■■■ 124.3 • 45.8h
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

Traveler Information Stolen in Eurail Data Breach

SecurityWeek • ■■■■ 98.2 • 22.9h
Hackers stole the personal and reservation information of people with a Eurail pass and those who made a seat reservation with the company. The post Traveler
Why it matters: data breach, breach.
https://www.securityweek.com/traveler-information-stolen-in-eurail-data-breach/

OTHER

Fortinet Fixes Critical FortiSIEM Flaw Allowing Unauthenticated Remote Code

The Hacker News • ■■■■ 99.9 • 43.5h
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

CYBER NEWSLETTER

Friday, Jan 16, 2026 • 07:23 UTC

THREAT PULSE

Zero-Days 3
Ransomware 0
Breaches 3
Phishing 0
Other 4

TOP 10

1. Cisco Patches Zero-Day RCE Exploited by China-Linked APT in Secure Email Gateways
2. Critical WordPress Modular DS Plugin Flaw Actively Exploited to Gain Admin Access
3. Microsoft Fixes 114 Windows Flaws in January 2026 Patch, One Actively Exploited
4. Critical flaw in AWS Console risked compromise of build environment
5. Fortinet Fixes Critical FortiSIEM Flaw Allowing Unauthenticated Remote Code
6. AWS CodeBuild Misconfiguration Exposed GitHub Repos to Potential Supply Chain Attacks
7. Central Maine Healthcare Data Breach Impacts 145,000 Individuals
8. Traveler Information Stolen in Eurail Data Breach
9. New ‘StackWarp’ Attack Threatens Confidential VMs on AMD Processors
10. New Vulnerability in n8n

Lookback: 72h • Ranked by risk

AWS CodeBuild Misconfiguration Exposed GitHub Repos to Potential Supply Chain

The Hacker News • ■■■■ 99.0 • 11.9h
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

New ‘StackWarp’ Attack Threatens Confidential VMs on AMD Processors

SecurityWeek • ■■■■ 83.9 • 13.4h
Researchers have disclosed technical details on a new AMD processor attack that allows remote code execution inside confidential VMs. The post New ‘StackWarp’
Why it matters: remote code execution, trusted source.
https://www.securityweek.com/new-stackwarp-attack-threatens-confidential-vms-on-amd-processors/

New Vulnerability in n8n

Schneier on Security • ■■■■ 83.5 • 19.3h
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