CYBER NEWSLETTER

Wednesday, Jan 14, 2026 • 05:45 UTC

THREAT PULSE

Zero-Days 2
Ransomware 1
Breaches 1
Phishing 0
Other 6

TOP 10

1. January 2026 Microsoft Patch Tuesday: Actively exploited zero day needs attention
2. After Goldman, JPMorgan Discloses Law Firm Data Breach
3. SAP’s January 2026 Security Updates Patch Critical Vulnerabilities
4. Microsoft Patches Exploited Windows Zero-Day, 111 Other Vulnerabilities
5. Ransomware-Banden erpressen Opfer mit Compliance-Verstößen
6. Cybersecurity risk will accelerate this year, fueled in part by AI, says World Economic Forum
7. Adobe Patches Critical Apache Tika Bug in ColdFusion
8. GoBruteforcer Botnet Targeting Crypto, Blockchain Projects
9. New Advanced Linux VoidLink Malware Targets Cloud and container Environments
10. ServiceNow Patches Critical AI Platform Flaw Allowing Unauthenticated User Impersonation

Lookback: 24h • Ranked by risk

ZERO-DAYS

January 2026 Microsoft Patch Tuesday: Actively exploited zero day needs attention

CSO Online • ■■■■ 124.0 • 3.9h
Eight critical vulnerabilities and an actively exploited zero day highlight Microsoft’s first Patch Tuesday announcements for 2026 . Most of the higher scoring
Why it matters: zero-day, actively exploited.
https://www.csoonline.com/article/4116437/january-2026-microsoft-patch-tuesday-actively-exploited-zero-day-needs-attention.html

BREACHES

After Goldman, JPMorgan Discloses Law Firm Data Breach

SecurityWeek • ■■■■ 96.1 • 12.6h
The law firm Fried Frank seems to be informing high-profile clients about a recent data security incident. The post After Goldman, JPMorgan Discloses Law Firm
Why it matters: data breach, breach.
https://www.securityweek.com/after-goldman-jpmorgan-discloses-law-firm-data-breach/

OTHER

SAP’s January 2026 Security Updates Patch Critical Vulnerabilities

SecurityWeek • ■■■■ 87.5 • 17.4h
SAP has released 17 security notes, including four that address critical SQL injection, RCE, and code injection vulnerabilities. The post SAP’s January 2026 Security
Why it matters: critical, rce.
https://www.securityweek.com/saps-january-2026-security-updates-patch-critical-vulnerabilities/

Microsoft Patches Exploited Windows Zero-Day, 111 Other Vulnerabilities

SecurityWeek • ■■■■ 87.4 • 10.0h
Two vulnerabilities patched this month by Microsoft were disclosed publicly before fixes were released. The post Microsoft Patches Exploited Windows Zero-Day, 111
Why it matters: zero-day, trusted source.
https://www.securityweek.com/microsoft-patches-exploited-windows-zero-day-111-other-vulnerabilities/

RANSOMWARE

Ransomware-Banden erpressen Opfer mit Compliance-Verstößen

CSO Online • ■■■■ 74.6 • 14.9h
Digitala World – shutterstock.com Ransomware-Attacken zählen nach wie vor zu den häufigsten Angriffsmethoden. Wie aktuelle Analysen zeigen, drohen Cyberbanden ihren
Why it matters: ransomware.
https://www.csoonline.com/article/4116135/ransomware-banden-erpressen-opfer-mit-compliance-verstosen.html

Cybersecurity risk will accelerate this year, fueled in part by AI, says World Economic

CSO Online • ■■■■ 72.8 • 8.9h
Cybersecurity risk will accelerate this year, fueled by advances in AI, deepening geopolitical fragmentation and the complexity of supply chains, the World Economic
Why it matters: supply chain, recent.
https://www.csoonline.com/article/4116270/cybersecurity-risk-will-accelerate-this-year-fueled-in-part-by-ai-says-world-economic-forum.html

Adobe Patches Critical Apache Tika Bug in ColdFusion

SecurityWeek • ■■■■ 67.4 • 9.9h
Adobe has released patches for 25 vulnerabilities across its products, including a critical Apache Tika flaw in ColdFusion. The post Adobe Patches Critical Apache Tika
Why it matters: critical, trusted source.
https://www.securityweek.com/adobe-patches-critical-apache-tika-bug-in-coldfusion/

CYBER NEWSLETTER

Wednesday, Jan 14, 2026 • 05:45 UTC

THREAT PULSE

Zero-Days 2
Ransomware 1
Breaches 1
Phishing 0
Other 6

TOP 10

Lookback: 24h • Ranked by risk

GoBruteforcer Botnet Targeting Crypto, Blockchain Projects

SecurityWeek • ■■■■ 66.2 • 12.4h
The botnet’s propagation is fueled by the AI-generated server deployments that use weak credentials, and legacy web stacks. The post GoBruteforcer Botnet Targeting
Why it matters: botnet, trusted source.
https://www.securityweek.com/gobruteforcer-botnet-targeting-crypto-blockchain-projects/

New Advanced Linux VoidLink Malware Targets Cloud and container Environments

The Hacker News • ■■■■ 62.1 • 17.8h
Cybersecurity researchers have disclosed details of a previously undocumented and feature-rich malware framework codenamed VoidLink that's specifically
Why it matters: malware, trusted source.
https://thehackernews.com/2026/01/new-advanced-linux-voidlink-malware.html

ServiceNow Patches Critical AI Platform Flaw Allowing Unauthenticated User Impersonation

The Hacker News • ■■■■ 62.0 • 18.0h
ServiceNow has disclosed details of a now-patched critical security flaw impacting its ServiceNow artificial intelligence (AI) Platform that could enable an
Why it matters: critical, trusted source.
https://thehackernews.com/2026/01/servicenow-patches-critical-ai-platform.html