

CYBER NEWSLETTER

Wednesday, Jan 14, 2026 • 19:30 UTC

THREAT PULSE

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

TOP 10

1. Microsoft Fixes 114 Windows Flaws in January 2026 Patch, One Actively Exploited
2. January 2026 Microsoft Patch Tuesday: Actively exploited zero day needs attention
3. Fortinet Fixes Critical FortiSIEM Flaw Allowing Unauthenticated Remote Code
4. Robo-Advisor Betterment Discloses Data Breach
5. Microsoft Patches Exploited Windows Zero-Day, 111 Other Vulnerabilities
6. FBI Flags Quishing Attacks From North Korean APT
7. Microsoft Starts 2026 With a Bang: A Freshly Exploited Zero-Day
8. Ransomware-Banden erpressen Opfer mit Compliance-Verstößen
9. SpyCloud Launches Supply Chain Solution to Combat Rising Third-Party Identity Threats
10. Patch Tuesday, January 2026 Edition

Lookback: 72h • Ranked by risk

ZERO-DAYS

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

The Hacker News • ■■■■ 129.1 • 9.9h
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 wild.
Why it matters: actively exploited, in the wild.
<https://thehackernews.com/2026/01/microsoft-fixes-114-windows-flaws-in.html>

Microsoft Starts 2026 With a Bang: A Freshly Exploited Zero-Day

Dark Reading • ■■■■ 83.2 • 22.3h
The vendor's first Patch Tuesday of the year also contains fixes for 112 CVEs, nearly double the amount from last month.
Why it matters: zero-day.
<https://www.darkreading.com/application-security/microsofts-starts-2026-bang-zero-day>

RANSOMWARE

Ransomware-Banden erpressen Opfer mit Compliance-Verstößen

CSO Online • ■■■■ 77.5 • 28.7h
Digitala World – shutterstock.com Ransomware-Attacken zählen nach wie vor zu den häufigsten Angriffsmethoden. Wie aktuelle Analysen zeigen, drohen Cyberbanden ihren Opfern mit Compliance-Verstößen.
Why it matters: ransomware.
<https://www.csoonline.com/article/4116135/ransomware-banden-erpressen-opfer-mit-compliance-verstosen.html>

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

CSO Online • ■■■■ 123.6 • 17.7h
Eight critical vulnerabilities and an actively exploited zero day highlight Microsoft's first Patch Tuesday announcements for 2026. Most of the higher scoring vulnerabilities have been actively exploited.
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>

Microsoft Patches Exploited Windows Zero-Day, 111 Other Vulnerabilities

SecurityWeek • ■■■■ 88.2 • 22.5h
Two vulnerabilities patched this month by Microsoft were disclosed publicly before fixes were released. The post Microsoft Patches Exploited Windows Zero-Day, 111 Other Vulnerabilities.
Why it matters: zero-day, trusted source.
<https://www.securityweek.com/microsoft-patches-exploited-windows-zero-day-111-other-vulnerabilities/>

BREACHES

Robo-Advisor Betterment Discloses Data Breach

SecurityWeek • ■■■■ 99.1 • 8.7h
A threat actor breached Betterment's systems, accessed customer information, and sent scam crypto-related messages. The post Robo-Advisor Betterment Discloses Data Breach.
Why it matters: data breach, breach.
<https://www.securityweek.com/robo-advisor-betterment-discloses-data-breach/>

PHISHING

CYBER NEWSLETTER

Wednesday, Jan 14, 2026 • 19:30 UTC

THREAT PULSE

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

TOP 10

1. Microsoft Fixes 114 Windows Flaws in January 2026 Patch, One Actively Exploited
2. January 2026 Microsoft Patch Tuesday: Actively exploited zero day needs attention
3. Fortinet Fixes Critical FortiSIEM Flaw Allowing Unauthenticated Remote Code
4. Robo-Advisor Betterment Discloses Data Breach
5. Microsoft Patches Exploited Windows Zero-Day, 111 Other Vulnerabilities
6. FBI Flags Quishing Attacks From North Korean APT
7. Microsoft Starts 2026 With a Bang: A Freshly Exploited Zero-Day
8. Ransomware-Banden erpressen Opfer mit Compliance-Verstößen
9. SpyCloud Launches Supply Chain Solution to Combat Rising Third-Party Identity Threats
10. Patch Tuesday, January 2026 Edition

Lookback: 72h • Ranked by risk

FBI Flags Quishing Attacks From North Korean APT

Dark Reading • ■■■■ 83.7 • 48.1h

A state-sponsored threat group tracked as "Kimsuky" sent QR-code-filled phishing emails to US and foreign government agencies, NGOs, and academic institutions.

Why it matters: apt, phishing.

<https://www.darkreading.com/mobile-security/fbi-quishing-attacks-north-korean-apt>

Patch Tuesday, January 2026 Edition

Krebs on Security • ■■■■ 73.5 • 18.7h

Microsoft today issued patches to plug at least 113 security holes in its various Windows operating systems and supported software. Eight of the vulnerabilities earned

Why it matters: critical, trusted source.

<https://krebsonsecurity.com/2026/01/patch-tuesday-january-2026-edition/>

OTHER

Fortinet Fixes Critical FortiSIEM Flaw Allowing Unauthenticated Remote Code

The Hacker News • ■■■■ 104.2 • 7.6h

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>

SpyCloud Launches Supply Chain Solution to Combat Rising Third-Party Identity Threats

CSO Online • ■■■■ 74.2 • 6.5h

SpyCloud, the leader in identity threat protection, today announced the launch of its Supply Chain Threat Protection solution, an advanced layer of defense that

Why it matters: supply chain, recent.

<https://www.csoonline.com/article/4116536/spycloud-launches-supply-chain-solution-to-combat-rising-third-party-identity-threats.html>