CYBER NEWSLETTER

Monday, Jan 12, 2026 • 19:15 UTC

THREAT PULSE

Zero-Days	0
Ransomware	0
Breaches	1
Phishing	0
Other	9

TOP 10

1. n8n Supply Chain Attack Abuses Community Nodes to Steal OAuth Tokens
2. Iran-linked MuddyWater APT deploys Rust-based implant in latest campaign
3. Shai-Hulud & Co.: Die Supply Chain als Achillesferse
4. Malicious npm packages target the n8n automation platform in a supply chain attack
5. GoBruteforcer Botnet Targets Crypto Project Databases by Exploiting Weak Credentials
6. Critical vulnerability found in n8n workflow automation platform
7. GoFundMe Ignores Own Rules by Hosting a Legal-Defense Fund for the ICE Agent Who
8. Cyber Insights 2026: What CISOs Can Expect in 2026 and Beyond
9. Instagram Fixes Password Reset Vulnerability Amid User Data Leak
10. ■ Weekly Recap: AI Automation Exploits, Telecom Espionage, Prompt Poaching & More

Lookback: 24h • Ranked by risk

BREACHES

GoFundMe Ignores Own Rules by Hosting a Legal-Defense Fund for the ICE Agent Who

WIRED Security • ■■■■ 61.4 • 0.5h

The fundraiser for the ICE agent in the Renee Good killing has stayed online in seeming breach of GoFundMe's own terms of service, prompting questions about selective

Why it matters: breach, breaking.

https://www.wired.com/story/gofundme-ice-jonathan-ross-renee-good-fundraiser/

Shai-Hulud & Co.: Die Supply Chain als Achillesferse

CSO Online • ■■■■ 73.8 • 4.8h

FAMArtPhotography – shutterstock.com Heutige Anwendungen basieren auf zahlreichen Komponenten, von denen jede zusammen mit den Entwicklungsumgebungen

Why it matters: supply chain, breaking.

https://www.csoonline.com/article/4115440/shai-hulud-co-die-supply-chain-als-achillesferse.html

Malicious npm packages target the n8n automation platform in a supply chain attack

CSO Online • ■■■■ 73.2 • 7.5h

Threat actors were spotted weaponizing the n8n automation ecosystem this week, slipping malicious npm packages into its marketplace of community-maintained

Why it matters: supply chain, recent.

https://www.csoonline.com/article/4115417/malicious-npm-packages-target-n8n-automation-platform-in-a-supply-chain-attack.html

Cyber Insights 2026: What CISOs Can Expect in 2026 and Beyond

SecurityWeek • ■■■■ 48.9 • 4.3h

Here we examine the CISO Outlook for 2026, with the purpose of evaluating what is happening now and preparing leaders for what lies ahead in 2026 and beyond.

Why it matters: trusted source, breaking.

https://www.securityweek.com/cyber-insights-2026-what-cisos-can-expect-in-2026-and-beyond/

OTHER

n8n Supply Chain Attack Abuses Community Nodes to Steal OAuth Tokens

The Hacker News • ■■■■ 79.2 • 2.6h

Threat actors have been observed uploading a set of eight packages on the npm registry that masqueraded as integrations targeting the n8n workflow automation

Why it matters: supply chain, trusted source.

https://thehackernews.com/2026/01/n8n-supply-chain-attack-abuses.html

Iran-linked MuddyWater APT deploys Rust-based implant in latest campaign

CSO Online • ■■■■ 77.6 • 9.4h

Iran-linked advanced persistent threat group MuddyWater has deployed a Rust-based implant in an ongoing espionage campaign targeting organizations in Israel and

Why it matters: apt, recent.

https://www.csoonline.com/article/4115379/iran-linked-muddywater-apt-deploys-rust-based-implant-in-latest-campaign.html

GoBruteforcer Botnet Targets Crypto Project Databases by Exploiting Weak Credentials

The Hacker News • ■■■■ 67.9 • 8.5h

A new wave of GoBruteforcer attacks has targeted databases of cryptocurrency and blockchain projects to co-opt them into a botnet that's capable of brute-forcing

Why it matters: botnet, trusted source.

https://thehackernews.com/2026/01/gobruteforcer-botnet-targets-crypto.html

Critical vulnerability found in n8n workflow automation platform

Cybersecurity Dive • ■■■■ 63.2 • 2.8h

The open-source platform is widely used across enterprise environments, leaving thousands of instances at risk.

Why it matters: critical, breaking.

https://www.cybersecuritydive.com/news/critical-vulnerability-n8n-automation-platform/809360/

CYBER NEWSLETTER

Monday, Jan 12, 2026 • 19:15 UTC

THREAT PULSE

Zero-Days	0
Ransomware	0
Breaches	1
Phishing	0
Other	9

TOP 10

1. n8n Supply Chain Attack Abuses Community Nodes to Steal OAuth Tokens
2. Iran-linked MuddyWater APT deploys Rust-based implant in latest campaign
3. Shai-Hulud & Co.: Die Supply Chain als Achillesferse
4. Malicious npm packages target the n8n automation platform in a supply chain attack
5. GoBruteforcer Botnet Targets Crypto Project Databases by Exploiting Weak Credentials
6. Critical vulnerability found in n8n workflow automation platform
7. GoFundMe Ignores Own Rules by Hosting a Legal-Defense Fund for the ICE Agent Who
8. Cyber Insights 2026: What CISOs Can Expect in 2026 and Beyond
9. Instagram Fixes Password Reset Vulnerability Amid User Data Leak
10. ■ Weekly Recap: AI Automation Exploits, Telecom Espionage, Prompt Poaching & More

Lookback: 24h • Ranked by risk

Instagram Fixes Password Reset Vulnerability Amid User Data Leak

SecurityWeek • ■■■■ 48.8 • 5.0h

The social media platform confirmed that the issue allowed third parties to send password reset emails to Instagram users. The post Instagram Fixes Password Reset

Why it matters: trusted source, breaking.

https://www.securityweek.com/instagram-fixes-password-reset-vulnerability-amid-user-data-leak/

■ Weekly Recap: AI Automation Exploits, Telecom Espionage, Prompt Poaching & More

The Hacker News • ■■■■ 48.7 • 5.6h

This week made one thing clear: small oversights can spiral fast. Tools meant to save time and reduce friction turned into easy entry points once basic safeguards were

Why it matters: trusted source, breaking.

https://thehackernews.com/2026/01/weekly-recap-ai-automation-exploits.html