



Hardening Critical Infrastructure Against Agentic AI Cyberattacks

Mirko Ross | 2026

asvin.io

Short Bio: Mirko Ross | CEO and Cybersecurity Expert

Published: 9. April 2025

Author: Christian Billmann



MR-IMG_3869_new

Mirko Ross – From Hacker to Internationally Recognized Expert in AI for Cybersecurity

Mirko Ross makes cybersecurity tangible.

Cybersecurity in the age of AI can be complex and abstract – but it doesn't have to be! As an internationally recognized expert, Mirko Ross not only brings in-depth technical expertise to the table but also knows how to get to the heart of the matter: **engaging, understandable, and captivating**. Whether speaking to a high-caliber technical audience or to management without a deep technical background.

About Mirko Ross

As founder and CEO of asvin.io, **Mirko Ross** is actively **shaping the future of cybersecurity under the motto "AI First."**

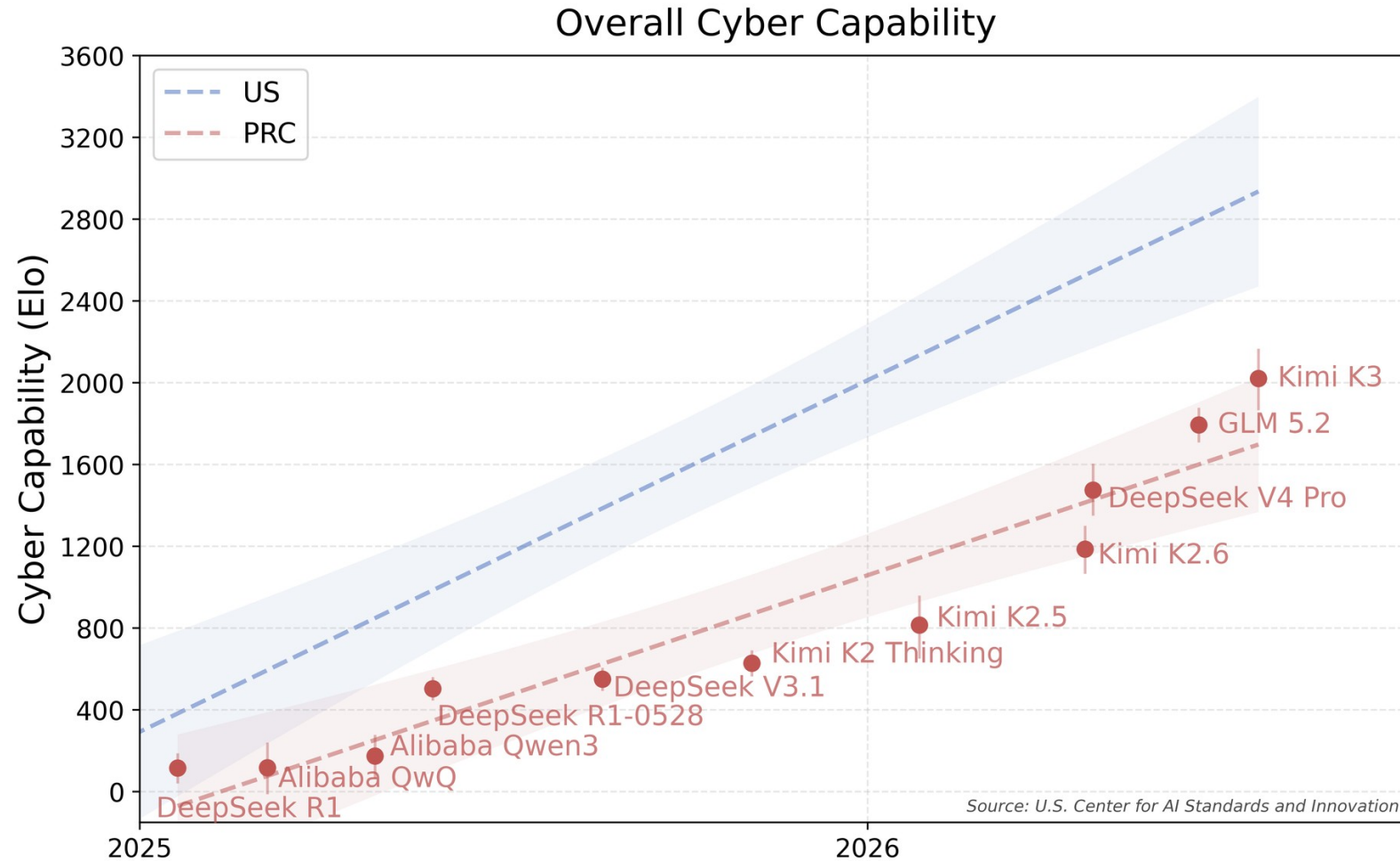
A hacker in his youth, he now shares his experience and knowledge to protect businesses, the government, and society from cyberattacks.

His expertise has led him to advisory bodies of the European Commission, the German Federal Government (**BMBF**), federal agencies (**Cyber Agency**), the German Bundestag, and the business community (**BDI**).

Companies and institutions benefit from his deep understanding of threat landscapes and **solutions** in the areas of cybersecurity, artificial intelligence (AI), and a digitally resilient society.

He is setting new standards particularly in the field of cyber risk analysis– with innovative approaches that not only uncover hidden risks but also actively reduce them using AI methods.

Open Weight Model Cyber Capability



Preliminary comparison of aggregate capabilities over time of the most capable U.S. and PRC models as of Kimi K3's release. <https://www.aisi.gov.uk/blog/preliminary-assessment-of-kimi-k3s-cyber-capabilities>

AI on Exploit Benchmark

	Top U.S. Models	Kimi K3	GLM-5.2
Full exploit <i>instruction-pointer control → ACE</i>	20	0	0
General primitives <i>cage-escape leak + arbitrary r/w</i>	30	0	0
V8 primitives <i>in-cage addrof / fakeobj / r-w</i>	38	17	6
Bug reproduction <i>trigger the bug (crash / ASAN)</i>	39	34	24
Coverage <i>reach vulnerable code</i>	41	41	41

ExploitBench is a public benchmark, developed by Carnegie Mellon University, that measures a model's ability to progress along the software exploitation ladder, including coverage and crash reproduction, arbitrary read/write, control flow hijack, and arbitrary code execution.

Detailed ExploitBench performance for Kimi K3 and other models. Darker shading indicates greater cyber capability. Each row represents a key milestone in the exploit development chain, and each cell shows the number of ExploitBench tasks for which the model(s) in question were able to reach that milestone. Source: <https://www.aisi.gov.uk/blog/preliminary-assessment-of-kimi-k3s-cyber-capabilities>

AI Impact on Cybersecurity

GAP between vulnerabilities found
and ability to fix = window of
opportunity for threat actors

Vulnerabilities
scanned by AI

Scaleability of traditional cybersecurity organizations

(t)



VULNERABILITIES

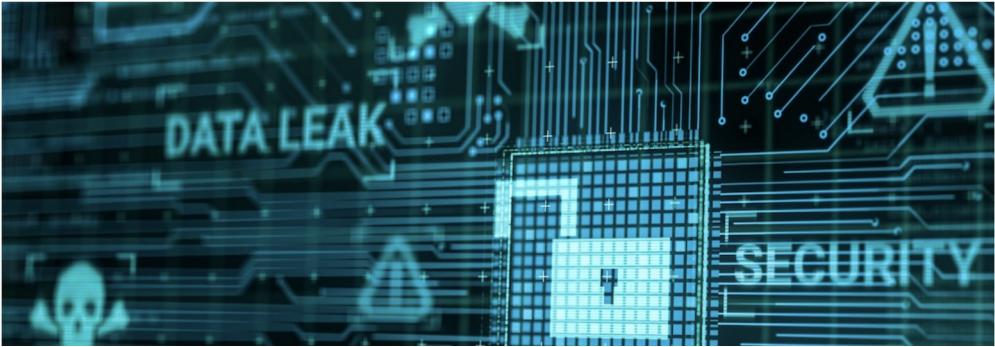
Critical JFrog Artifactory Vulnerability Reportedly Exploited in the Wild

Exploitation of the authentication bypass vulnerability CVE-2026-82329 started just days after its public disclosure.



By [Eduard Kovacs](#) | September 1, 2026 (5:59 AM ET)
Updated: September 2, 2026 (3:00 AM ET)





Latency in the Supply Chain:

26. Juni: Zero Day Exploit by AI Agents in the OpenAI Sandbox (Huggingface)

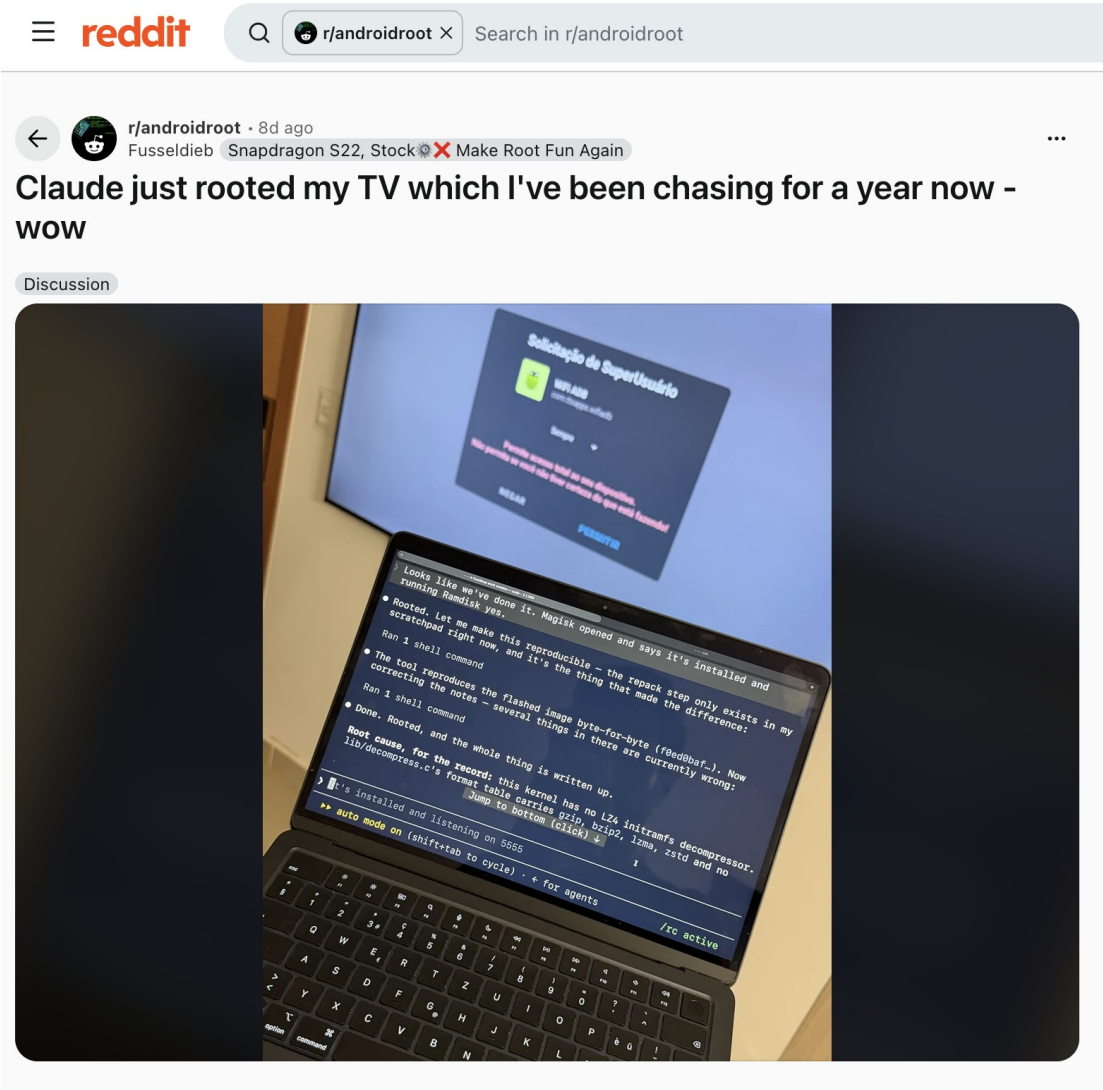
04. Juli: OpenAI detects Security Incident in Jfrog Artifactory

06. Juli: OpenAI informs Jfrog

27. Juli: JFrog publication of CVE

30. Juli: Artifactory Mass Exploitation

Rouge AI becomes a commodity



Hacking is a matter of
model / tool availability
not of human skills.

10 Measures to Secure Infrastructure Against Agentic AI Cyberattacks

- 1 Network Segmentation
- 2 Hardware Trusted Security (PUFs...)
- 3 Application Hygiene (Test & Production)
- 4 Monitoring & Anomaly Detection
- 5 Risk based Patching
- 6 Less Human in the Loop – more AI oversight
- 7 Zero Trust including Non Human Identities
- 8 AI augmented triage for SOC's
- 9 Persistent logging for forensic and monitoring
- 10 Pro active AI automated threat hunting



THANK YOU FOR YOUR TIME



Mirko Ross

CEO

m.ross@asvin.io

asvin GmbH

Stuttgart, Germany

www.asvin.io

contact@asvin.io