New CIS Report Warns Prompt Injection Attacks Pose Growing Risk to Generative AI

CLIFTON PARK, NY, UNITED STATES, April 1, 2026 /EINPresswire.com/ -- The Center for Internet Security, Inc. (CIS®) has released a new report warning that prompt injection attacks are a serious and growing threat to organizations using generative artificial intelligence (GenAI).

The report, Prompt Injections: The Inherent Threat to Generative AI, explains how cyber threat actors can manipulate AI systems by hiding malicious instructions in documents, emails, websites, and other data that AI tools are allowed to access. Those hidden instructions can lead to stolen sensitive data, unauthorized system access, and disrupted operations.

> This report makes clear that technical prompt injections aren't a theoretical problem, they're a real and immediate risk."
>
> *TJ Sayers, Senior Director of Threat Intelligence at CIS*

Prompt injection attacks take advantage of a basic limitation in current large language models: they cannot reliably tell the difference between legitimate instructions and malicious ones. As more organizations, including state and local governments, integrate AI tools into daily work, the risk from these attacks increases.

The report highlights real world examples where attackers used prompt injections to:

- Steal sensitive data, including credentials and internal documents
- Manipulate AI tools to perform unauthorized actions
- Poison AI systems so malicious instructions persist and spread over time

Recent research shows that these attacks often require little technical skill and can be difficult to detect with traditional security tools.

"This report makes clear that technical prompt injections aren't a theoretical problem; they're a real and immediate risk," said TJ Sayers, Senior Director of Threat Intelligence at the CIS. "As organizations race to adopt AI, attackers are finding novel ways to turn these tools against us,

including treating them as the newest front for 'living off the land' techniques. The good news is that there are concrete steps organizations can take now to reduce their exposure and use AI more safely."

The report stresses that protecting GenAI systems requires more than just securing the AI model itself. Organizations must also carefully control what data and systems AI tools can access and ensure humans remain involved in high risk actions.

CIS recommends organizations take the following key actions:

- Establish clear rules for how and when employees can use GenAI tools
- Limit AI's access to sensitive systems and data using the principle of least privilege
- Require human approval before AI tools can execute code or make high impact changes like data erasure
- Maintain inventories of the data, systems, and tools AI platforms can access
- Train staff to recognize emerging AI related security risks, including prompt injection attacks
- Incorporate AI technology security assessments into penetration testing plans

Join CIS leaders for a discussion of the report, its findings, and recommendations on an upcoming podcast episode of Cybersecurity Where You Are, to be released on April 29.

To learn more about Penetration Testing Services, please reach out to services@cisecurity.org.

For additional information or media requests, please contact media@cisecurity.org.

###

About CIS
The Center for Internet Security, Inc. (CIS®) makes the connected world a safer place for people, businesses, and governments through our core competencies of collaboration and innovation. We are a community-driven nonprofit, responsible for the CIS Critical Security Controls® and CIS Benchmarks® guidelines, globally recognized best practices for securing IT systems and data. We lead a global community of IT professionals to continuously evolve these standards and provide products and services to proactively safeguard against emerging threats. Our CIS Hardened Images® provide secure, on-demand, scalable computing environments in the cloud. CIS is home to the Multi-State Information Sharing and Analysis Center® (MS-ISAC®) organization, the trusted resource for cyber threat prevention, protection, response, and recovery for U.S. State, Local, Tribal, and Territorial government entities, and the Elections Infrastructure Information Sharing and Analysis Center® (EI-ISAC®) organization, which supports the rapidly changing cybersecurity needs of U.S. election offices To learn more, visit cisecurity.org or follow us on X: @CISecurity.

Kelly Wyland
Center for Internet Security

+1 518-256-6978
email us here
Visit us on social media:
LinkedIn
Instagram
Facebook
YouTube
X
