

ProCircular Research Demonstrates How Prompt Injection Can Compromise AI Voice Agents at DEF CON 34

ProCircular's Willie Zhang reveals at DEF CON 34 how prompt injection can hijack AI voice agents, exposing new enterprise security risks



DES MOINES, IA, UNITED STATES,
August 4, 2026 /EINPresswire.com/ --

[ProCircular](#), a leading cybersecurity consulting and managed security services provider, today announced that Offensive Security Consultant Willie Zhang will present original research at DEF CON 34 examining how prompt injection attacks can be used to manipulate AI-powered voice agents, exposing a rapidly emerging security challenge as organizations increasingly adopt conversational AI.

AI voice agents are quickly moving beyond customer service into help desks, IT operations, employee support, healthcare, financial services, and other enterprise workflows. While these systems promise greater efficiency, they also create new opportunities for attackers to influence AI behavior, bypass intended safeguards, and manipulate automated decision-making through carefully crafted prompts delivered in natural language.

During his DEF CON presentation, "For Prompt Injection, Press 1: Hacking AI Voice Agents," Zhang will demonstrate how prompt injection techniques extend beyond text-based large language models into voice-enabled AI systems. The session explores how attackers can exploit these interactions, the security risks organizations should understand before deploying AI voice agents at scale, and practical considerations for reducing enterprise exposure.

"As organizations rapidly integrate AI voice agents into business operations, security needs to evolve just as quickly," said Willie Zhang, Offensive Security Consultant at ProCircular. "Voice interfaces introduce another pathway for interacting with AI systems, and organizations should understand how prompt injection and related attacks may affect these deployments."

The presentation reflects ProCircular's continued investment in [offensive security research](#) that helps organizations anticipate emerging threats before they become widespread. By combining penetration testing, adversary simulation, and real-world attack research, the company helps

organizations identify weaknesses in modern technologies, including AI systems, before adversaries can exploit them.

Presentation Details

Conference: DEF CON 34

Session: For Prompt Injection, Press 1: Hacking AI Voice Agents

Speaker: Willie Zhang, Offensive Security Consultant, ProCircular

Location: Social Engineering Community Village; Room W317 - W319

Date/Time: August 8, 2:00 pm PT

Available for Interviews

Willie Zhang is available during DEF CON to discuss:

Prompt injection attacks against AI voice agents

Offensive security testing for AI applications

Securing enterprise AI and agentic AI deployments

Emerging AI attack techniques and enterprise risk

Best practices for evaluating AI system security

About ProCircular

ProCircular is a cybersecurity firm that helps organizations see where they're vulnerable, understand how those gaps get exploited, and build a security program grounded in the real world. We invest in advanced cybersecurity and AI research, then translate complex findings into practical guidance and solutions our clients can actually use. Across assessments, monitoring, incident response, advisory, AI risk, and compliance, ProCircular brings deep technical expertise, practical judgment, and a team that stays involved from initial findings through response and longer-term program development.

Trusted by organizations across healthcare, finance, manufacturing, education, transportation and logistics, and government, where downtime and risk carry real operational weight, ProCircular helps teams move from reactive security work to confident decisions, stronger readiness, and better follow-through. Learn more at ProCircular.com.

Kari Ritacco

RedIron PR

kari@redironpr.com

This press release can be viewed online at: <https://www.einpresswire.com/article/931504622>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

