

Note: This document has been translated from the Japanese original for reference purposes only. In the event of any discrepancy between this translated document and the Japanese original, the original shall prevail.

July 23, 2026
DIGITAL HEARTS HOLDINGS Co., Ltd.

AGEST Commences PoC for Commercialization of Autonomous AI-Driven Comprehensive Cybersecurity Platform “AGEST ZERO SHIELD” Co-Developed with U.S.-Based Lazarus



DIGITAL HEARTS HOLDINGS Co., Ltd. hereby announces that AGEST Inc. (hereinafter referred to as “AGEST”), our consolidated subsidiary that supports the improvement of software quality and safety utilizing advanced quality technologies, will commence a Proof of Concept (PoC) from the end of July 2026 toward the commercialization of the “Autonomous AI-Driven Comprehensive Cybersecurity Platform” co-developed with U.S.-based Lazarus Enterprises, Inc. (“Lazarus”), as previously announced on June 10, 2026.

<Recent Cybersecurity Trends and Challenges Facing Companies and Organizations>

With the emergence of advanced AI frontier models, exemplified by the recently announced “Claude Mythos Preview” (hereinafter “Mythos”) *1, the environment surrounding cybersecurity is undergoing significant changes, including the sophistication of both AI-driven attacks and defenses.

DIGITAL HEARTS HOLDINGS Co., Ltd.

Tokyo Opera City Bldg. 41F, 3-20-2 Nishi-Shinjuku, Shinjuku-ku, Tokyo
163-1441, Japan
<https://en.digitalhearts-hd.com/>

From the defensive perspective of companies and organizations, continuously strengthening defensive capabilities against these new cyber threats has become a critical management issue underpinning business continuity and corporate trust.

On the other hand, security measures utilizing advanced AI models entail challenges such as:

- External transmission risk of source code via APIs (data sovereignty concerns)
- Heavy token billing burdens due to a rapid increase in traffic, such as increased full-scan opportunities
- Condition hurdles for utilizing frontier AI models like Mythos, as well as the risk of sudden service suspension due to export regulations, etc.
- The need to respond to high-speed and high-frequency alerts, leading to alert fatigue risks

Furthermore, while attackers utilize advanced AI, defensive entities such as companies and organizations are hindered by multiple layers of safety measures (guardrails). This creates a concern regarding an asymmetry where code verification from an attacker's perspective cannot progress through legitimate procedures.

<About “AGEST ZERO SHIELD” and the Start of the PoC>

To continuously resolve these challenges, the AGEST has co-developed the “Autonomous AI-Driven Comprehensive Cybersecurity Platform ‘AGEST ZERO SHIELD’” with Lazarus. As the first phase, we are preparing for the commercialization in September 2026 of the “Zero-Day Vulnerability Hunting” feature, which includes zero-day vulnerability detection similar to frontier AI and a function to propose patches or code fixes for discovered vulnerabilities.

Features of ‘AGEST ZERO SHIELD’

- Can be utilized while ensuring data sovereignty through installation in on-premises/closed-network environments.

* Unlike frontier AI, source code is not transmitted to overseas companies.

- An annual fixed-fee license system, not token-based.
- Planned continuous version upgrades for AI models specifically specialized in cybersecurity.

Additionally, it boasts high vulnerability hunting capabilities achieved through a proprietary harness and LLM tuning by Lazarus and the AGEST. In AGEST’s verifications, it has successfully discovered vulnerabilities such as the “FFmpeg H.264 slice counter vulnerability” *2 (also cited as an example by Mythos), as well as previously undiscovered vulnerabilities, such as the following examples.

DIGITAL HEARTS HOLDINGS Co., Ltd.

Tokyo Opera City Bldg. 41F, 3-20-2 Nishi-Shinjuku, Shinjuku-ku, Tokyo

163-1441, Japan

<https://en.digitalhearts-hd.com/>

■ Examples of Actually Detected Vulnerabilities

CVE	ANT-CVD	Date	CVSS	Lang	Description
CVE-2026-28208	ANT-2026-9VJ9JXQ	2026/2/26	5.9	Java	Junrar has arbitrary file write due to backslash path traversal bypass in LocalFolderExtractor on Linux/Unix
CVE-2026-32316	ANT-2026-EBDTPNVH	2026/4/13	7.5	C	jq: Integer overflow in jvp_string_append() allows Heap-based Buffer Overflow
CVE-2026-40034	ANT-2026-6SNS6KMP	2026/5/26	7.3	Rust	gitoxide - Command Injection via Partial .gitmodules Override in gix-submodule
CVE-2026-27775	-	2026/7/3	8.8	Go	Gitea pre-receive hook permission cache allows full repository write access

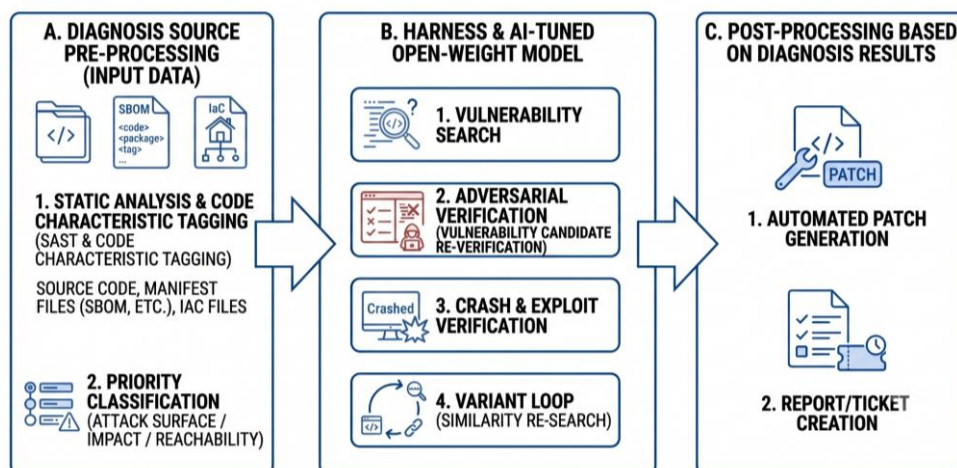
*CVE: CVE (Common Vulnerabilities and Exposures) is a universal identification number assigned to publicly known security vulnerabilities (flaws) in systems and software.

*ANT CVD: Coordinated Vulnerability Disclosure (CVD) identification number, a system for properly fixing and publishing vulnerabilities. When Anthropic PBC discovers a vulnerability, an ANT identifier is assigned, though it may not always be published as standalone vulnerability information.

*CVSS: CVSS (Common Vulnerability Scoring System) is an international industry standard metric that quantifies the severity of security vulnerabilities in information systems and software on a scale of 0.0 to 10.0. A higher score indicates a higher risk level, and it is utilized by organizations to prioritize vulnerability responses.

Exploit Chain Context: In recent years, a cyberattack method known as an “Exploit Chain” has emerged, where attackers sequentially chain execution of attack codes against multiple vulnerabilities (security holes) to achieve an ultimate goal, such as seizing control of a system. Even if individual vulnerabilities present a low-level threat on their own, cleverly combining them has revealed attack methods that can ultimately hijack privileges at the deepest levels of a system. Consequently, threat levels can no longer be judged solely by CVSS scores.

■ Flow of Zero-Day Vulnerability Hunting



Each process is looped multiple times to suppress hallucinations and ensure improved reproducibility.

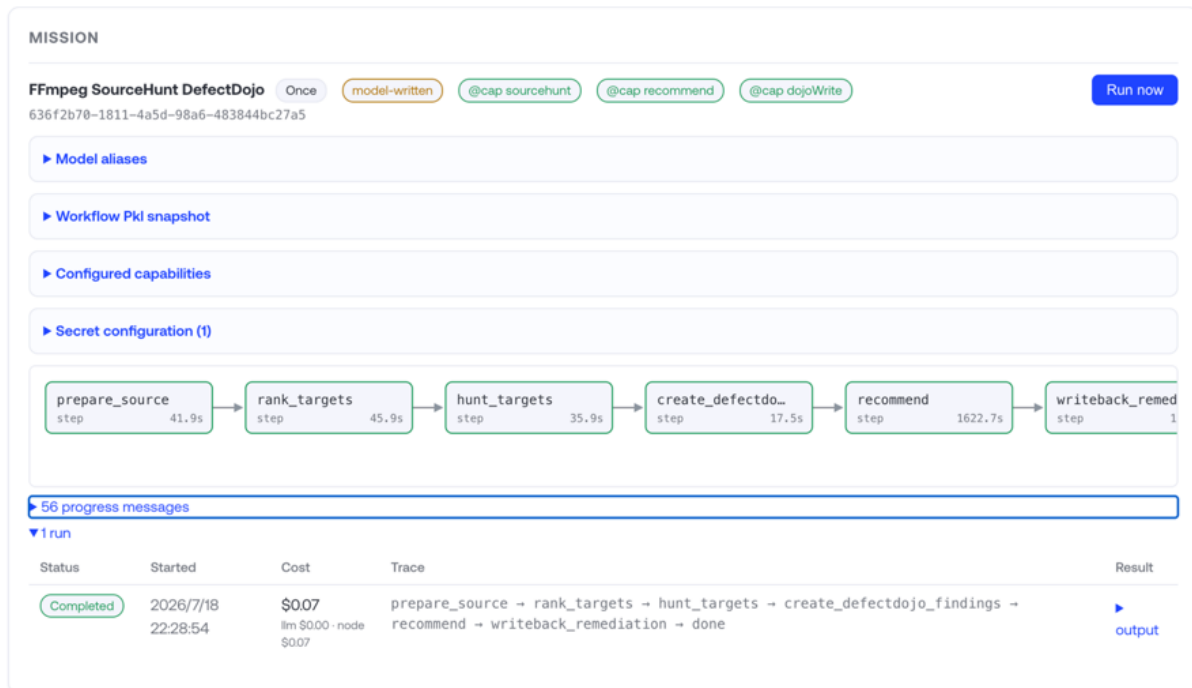
DIGITAL HEARTS HOLDINGS Co., Ltd.

Tokyo Opera City Bldg. 41F, 3-20-2 Nishi-Shinjuku, Shinjuku-ku, Tokyo

163-1441, Japan

<https://en.digitalhearts-hd.com/>

■ Image of the Vulnerability Detection Screen



To introduce these results into actual customer environments and conduct various verifications toward commercialization, the AGEST will commence PoCs from the end of this month with partner companies, centered around major domestic SIers with whom we have been in discussions.

<Future Initiatives>

Having received numerous inquiries from various companies, AGEST has already closed the application period for this upcoming PoC. Moving forward, AGEST will engage in ongoing discussions regarding the execution of this PoC and its commercialization, and proceed with the construction of a partnership ecosystem with deployment consulting partners and hardware procurement partners to widely promote the introduction of "AGEST ZERO SHIELD."

Details such as the commercialization schedule and additional features will be publicly announced in due course.

Planned Additional Features

- Live target monitoring function (equivalent to CNAP)
- Detection of security breaches through log analysis of live targets
- Autonomous AI penetration testing
- Offensive cyber control functions

*1: An advanced AI model provided on a limited basis by Anthropic PBC, particularly a frontier model specialized in the cybersecurity domain, such as zero-day vulnerability detection, vulnerability analysis, and attack path generation.

DIGITAL HEARTS HOLDINGS Co., Ltd.

Tokyo Opera City Bldg. 41F, 3-20-2 Nishi-Shinjuku, Shinjuku-ku, Tokyo
163-1441, Japan
<https://en.digitalhearts-hd.com/>

*2: As a result of Project Glasswing, this detected a vulnerability that had laid hidden in the FFmpeg H.264 slice counter for 16 years (An issue called "h.264 slice counter mismatch or 0xFFFF sentinel collision", for which no CVE number has been issued).

* All brands, product names, company names, trademarks and service marks are the properties of their respective owners.

【About AGEST, Inc.】

Through the provision of software testing services and security services, AGEST aims to contribute to improving the quality of our customers' products and the development of an advanced digital society.

<https://agest.co.jp>

【Inquiries from the media】

AGEST, Inc. IR & PR Department, PR Representative

Mail: ml-pr@agest.co.jp

Tel: 03-6821-1753

DIGITAL HEARTS HOLDINGS Co., Ltd.

Tokyo Opera City Bldg. 41F, 3-20-2 Nishi-Shinjuku, Shinjuku-ku, Tokyo
163-1441, Japan

<https://en.digitalhearts-hd.com/>