MOBASI

Initiatives / Sentinel

Sentinel

Securing open-source digital forensics tools

Digital forensics investigators rely on open-source tools every day. These tools process sensitive evidence, parse complex file formats, and help solve crimes. Yet many have never received a professional security review.

Through our **Sentinel** program, Mobasi performs security reviews for open-source forensics tools. Our team identifies vulnerabilities, documents findings, and works with maintainers through responsible disclosure to resolve issues before they can be exploited.

We are systematically reviewing tools in the digital forensic ecosystem to identify vulnerabilities and improve security. If you'd like your tool to be included or accelerated, please reach out below.

Our review process

- Deep code review for security vulnerabilities
- Dependency analysis and supply chain reviews
- Coordinated responsible disclosure with maintainers
- Pull requests with fixes where appropriate
- Public recognition for participating projects

MOBASI

Since launching Sentinel, we've identified multiple critical and high-severity vulnerabilities across widely-used forensics tools. We work closely with maintainers to ensure issues are addressed before public disclosure.

Vulnerability index

Tool	Type	Severity	Date
Sleuth Kit	tsk_recover Path Traversal	HIGH	2026-03-05
Sleuth Kit	APFS Keybag Parser OOB Read	MEDIUM	2026-03-05
Sleuth Kit	ISO9660 SUSP ER Length Trust OOB Read	MEDIUM	2026-03-05
ALEAPP	NQ Vault Path Traversal / RCE	CRITICAL	2026-03-05
NSA Ghidra	Arbitrary Code Execution via @execute Annotation	HIGH	2026-02-20
Hayabusa	XSS from HTML Inputs	HIGH	2026-02-20
parseusbs	Command Injection via LNK Filename	CRITICAL	2026-02-20
parseusbs	Command Injection via -v Volume Argument	HIGH	2026-02-20
unfurl	Permanent Debug Mode	CRITICAL	2026-01-28

MOBASI

Tool	Type	Severity	Date
bulk_extractor	Heap Overflow Attack	HIGH	2026-01-28
unfurl	Decompression Bomb DoS	MEDIUM	2026-01-28
tcpflow	Out of Bounds Write	MEDIUM	2026-02-20
MemProcFS	Python Plugin Loader Hijack	HIGH	2026-02-20
UAC	Eval Command Injection in _run_command	CRITICAL	2026-04-05
UAC	Command Injection via command_collector	HIGH	2026-04-05
UAC	User Home Placeholder Injection from passwd	HIGH	2026-04-05

Some vulnerabilities remain under embargo during responsible disclosure. This table is updated as disclosures are made public.

Submit a tool for review

Maintain an open-source forensics tool? We'd like to help ensure it's secure. Submit your tool for consideration in our review program.

Submit a tool for review

MOBASI

Company

About

Careers

Product

Agent

Use Cases

Initiatives

Sentinel

Armory

Contact

contact@mobasi.ai

Austin, Texas

SOC 2 Type II Certified