

## Researchers: Forensics Software Can Be Hacked

The software that police and others use to investigate wrongdoing on computers could be more secure.

**Robert McMillan, IDG News Service**

Wednesday, July 25, 2007 07:00 AM PDT

The software that police and enterprise security teams use to investigate wrongdoing on computers is not as secure as it should be, according to researchers with Isec Partners Inc.

The San Francisco security company has spent the past six months investigating two forensic investigation programs, Guidance Software Inc.'s EnCase, and an open-source product called The Sleuth Kit. They have discovered about a dozen bugs that could be used to crash the programs or possibly even install unauthorized software on an investigator's machine, according to Alex Stamos, a researcher and founding partner with Isec Partners.

Researchers have been hacking forensics tools for years, but have traditionally focused on techniques that intruders could use to cover their tracks and thwart forensic investigations. The Isec team has taken a different tack, however, creating hacking tools that can be used to pound the software with data, looking for flaws.

Based on their findings, Stamos's team believes that the EnCase software is not written as securely as it should and could theoretically be exploited by an attacker.

"What Guidance needs to do is change their production and their quality assurance practices," Stamos said. "We looked at a small portion of the functionality of EnCase and we found that there are lots of bug that can make it impossible for somebody to complete their work," he said. "Basically we can make it impossible to open up a hard drive and look at it."

Isec is holding the technical details of its findings close to its chest, and is not saying whether any bugs they found could be exploited to do something much worse: install unauthorized software on a PC.

But the team will be disclosing some information at next week's [Black Hat](#) conference in Las Vegas, Stamos said.

What exactly will be disclosed? The Sleuth Kit project has already patched the flaws Isec has found, so those flaws will be made public. Details on EnCase may be released if the product is patched by then, Stamos said. Isec will also release the debugging and "fuzzing" tools it used to find these flaws, he added.

The Isec research looks interesting, but will probably not have a major impact on the lives of forensic researchers, said Jim Butterworth, Guidance's director of incident response.

Because forensic systems are typically not connected to external networks, they cannot be remotely controlled via the Internet, he said. So even if an attacker could use these techniques to compromise one forensic snapshot of a system, a second forensic tool would provide the real picture. "It's just not the big of a threat because I know a lot of other mitigating steps to take," he said. "A well-trained person does not use a single tool."

Another forensic researcher agreed that the Isec Partners research is interesting, but of limited use to criminals.

That's because most serious attackers are already good enough at covering their tracks that they will never be caught, according to James C. Foster, president and chief scientist at Ciphent Inc. "If you're an attacker you can basically beat the system," he said. "In my opinion, the bigger problem is that the product is not going to provide the data that you want."

However, there is one group that may pay special attention to the Stamos team: defense lawyers. If Isec shows that unauthorized software could have been run on an investigator's PC, it could ultimately undermine the usefulness of these forensic tools in court, said Chris Ridder, residential fellow at the Stanford University Law School Center for Internet and Society.

"The big risk is for someone to execute arbitrary code," he said. "If there's a risk that the evidence has been compromised or if something has been planted by a third party... then you can call into question the accuracy of the software and possibly get it thrown out."

Butterworth, who has been grilled many times by defense lawyers, agreed. "I wouldn't put anything past a defense attorney," he said.