Whistleblower vindicated in Cisco cybersecurity case

August 1 2019, by Frank Bajak

This July 30, 2019, photo provided by James Glenn shows Glenn, a computer security expert. Glenn won a trailblazing payout in a whistleblower lawsuit over critical security flaws he found in October 2008 in Cisco Systems Inc. video surveillance software used at major U.S. international airports and multiple federal agencies with sensitive missions thought his discovery would be a career-boosting milestone. (James Glenn via AP)

A computer security expert who has won a trailblazing payout in a whistleblower lawsuit over critical security flaws he found in October 2008 in Cisco Systems Inc. video surveillance software thought his discovery would be a career-boosting milestone.

James Glenn imagined at the time that Cisco would credit him on its website. The software was, after all, used at major U.S. international airports and multiple federal agencies with sensitive missions

"I mean, this was a pretty decent accomplishment," Glenn said Thursday in a phone interview.

Instead, he was fired by the Cisco reseller in Denmark that employed him, which cited cost-cutting needs. And Cisco kept the flaws in its Video Surveillance Manager system quiet for five years.

Only Wednesday, when an $8.6 million settlement was announced and the lawsuit he filed in 2011 under the federal False Claims Act unsealed, was Glenn's ordeal revealed—along with the potential peril posed by Cisco's long silence.

The law lets whistleblowers report fraud and misconduct in federal contracting—for selling flawed products, essentially—and collect financial rewards when claims succeed. Glenn's attorneys said his is the first cybersecurity case successfully litigated under the FCA.

Cybersecurity expert Chris Wysopal of Veracode said the case breaks new ground by making it clear that security vulnerabilities now fall into the flawed product category.

"This allows for a new type of bug bounty for security researchers if vendors drag their feet, continue selling their products to governments without notifying of the risk they know about and not fixing their flaws,"

he said.

The exploit Glenn, 42, discovered would have given an attacker full administrative access to the software that managed video feeds, letting them be monitored from a single location, the lawsuit says. It could also potentially allow unauthorized access to sensitive connected systems.

That meant an intruder might have taken control of or bypassed physical security systems such as locks and fire alarms, which are regularly connected to camera systems.

"An unauthorized user could effectively shut down an entire airport by taking control of all security cameras and turning them off," the suit says. Airports affected included Los Angeles International and Chicago's Midway, it says.

"You could penetrate the entire system. And you could do that without any trace. And have complete backdoor access to the system whenever you wanted," said Michael Ronickher, an attorney representing Glenn with the firm Constantine Cannon LLP.

In this Oct. 3, 2018, file photo, the Cisco logo appears on a screen at the Nasdaq MarketSite in New York's Times Square. Computer security expert James Glenn won a rare payout in a whistleblower lawsuit he filed against Cisco Systems Inc. almost a decade ago, after he reported critical security flaws in Cisco video surveillance software used at major U.S. international airports and federal agencies with critical national security roles. Rather than being rewarded for his 2008 discovery, Glenn lost his job, according to the lawsuit he filed under the federal False Claims Act, which was unsealed Wednesday, July 31, 2019, with the announcement of an $8.6 million settlement. (AP Photo/Richard Drew, File)

The software was also used by the Department of Defense Biometrics Task Force Headquarters, the U.S. Secret Service, the Department of Homeland Security, the Army, the Navy, the Marine Corps, the National Aeronautics and Space Administration and the Federal Emergency Management Agency—as well as police stations, prisons, schools and by

Amtrak at its stations, the lawsuit says.

"I feel vindicated, but not in the celebratory sense," said Glenn, who gets 20% of the settlement payout, with the rest going to the federal government, 15 states and the District of Columbia.

"I think in terms of the punishment level for the other party maybe it's not that significant," he added.

Cisco issued a statement Wednesday saying it was "pleased to have resolved" the dispute and that "there was no allegation or evidence that any unauthorized access to customers' video occurred" as a result of the product's architecture. But it added that video feeds could "theoretically have been subject to hacking."

Ronickher, Glenn's lawyer, noted that the suit does not address all the international locations that bought the Cisco software, which he said include the Auckland airport, New Zealand's largest.

When Glenn discovered the flaws, he immediately alerted Cisco, but the U.S. technology giant did not acknowledge them until 2013, when it issued a security alert about "multiple security vulnerabilities " in the software.

That notice came two years after federal authorities began investigating.

The reseller, NetDesign, fired Glenn in March 2009, his lawyers say.

Two years later, after Glenn's sister notified the FBI and the lawsuit was filed claiming Cisco had defrauded U.S. federal, state and local governments who purchased the software system.

On July 22, the plaintiffs settled with Cisco in a case brought in New

York's Western District.

Glenn's lawyers and Cisco both announced the $8.6 million settlement amount the plaintiffs are due.

Glenn, the son of a Marine originally from Virginia, now lives in Bulgaria and has been working for the same company since 2011, which he declined to name.

He said he is married, with one child.