

1 July 2009

By: Lucian Constantin, Web News Editor



ATM vendor pressures Juniper into keeping its employee silent about ATM vulnerability
OneStopATM

[Upcoming ATM Hack Demo at Black Hat Gets Canceled](#)

Juniper stops its employee from going public at the request of ATM vendor

An intriguing and much expected presentation of a serious vulnerability affecting automated teller machines that was scheduled to take place at the upcoming Black Hat conference got canceled. The researcher was forced by its employer, Juniper Networks, to postpone making his findings public, following a request from the affected ATM vendor.

Security researcher Barnaby Jack was preparing a live demonstration on how to force an unmodified, stock ATM to release all of its cash by leveraging on a newly discovered vulnerability. This was part of his Black Hat scheduled talk called "Jackpotting Automated Teller Machines."

The researcher's employer, security and networking device manufacturer Juniper Networks, initially supported his intentions of disclosing the vulnerability publicly, [Risky.Biz reports](#). "Juniper believes that Jack's research is important to be presented in a public forum in order to advance the state of security," the company said in a statement.

However, facing pressure from the affected ATM vendor, which was reportedly notified in advance of the vulnerability and the presentation, Juniper forced its employee to cancel the talk for the time being. "The affected ATM vendor has expressed to us concern about publicly disclosing the research findings before its constituents were fully protected," the company explained.

Some of the main reasons behind the decision are suspicions that the issue might affect other ATM vendors as well. "Considering the scope and possible exposure of this issue on other vendors, Juniper decided to postpone Jack's presentation until all affected vendors have sufficiently addressed the issues found in his research," the company noted.

Security researchers from Trustwave have recently announced the existence of ATM malware that allows attackers to eject the cash-dispensing cassette, however, infecting the machine requires an insider, like a technician. Barnaby Jack's presentation promised to "explore both local and remote attack vectors."

This is not the first time when a security researcher is pressured into canceling a presentation. Back in 2007, Chris Paget, then a security researcher at IOActive, was pressured into canceling his Black Hat conference presentation about a vulnerability in RFID tags manufactured by a company called HID. The company threatened to sue for patent violation.

More recently, in 2008, the Massachusetts Bay Transit Authority [obtained](#) a restraining order against three MIT students planning to demonstrate how to hack the CharlieCard subway ticketing system at DEFCON. The gag order was later [lifted](#) by another judge.