Uninvited access to security camera systems pinned down

January 29 2013, by Nancy Owano

(Phys.org)—A digital video recorder (DVR), used in homes and businesses for security, is helpful when not in the hands of criminals, The latter scenario is what is rattling some security blog and *Forbes* readers, with the recent Forbes report by Andy Greenberg of how criminals are capable of hijacking security cameras. Once in control, surveillance camera footage can be played back, copied, deleted, or changed. The hijackers can also use the machines to access other computers behind the victim's firewall.

The findings come from two security-watching quarters pointing to design flaws that affect over 12 DVR brands studied.

One of those security sources, Rapid7, identified hackable video boxes using firmware provided by a China-based firm. Outside Rapid 7, a blogger, who declined to give Forbes his real name, had succeeded in disassembling a device and had run tests on it, finding that commands sent to the device via a port 9000 connection were accepted without authentication. He could use the connection to retrieve login credentials for the DVR's web-based control panel. "A whole slew of security dvr [sic] devices are vulnerable to an unauthenticated login disclosure and unauthenticated command injection."

HD Moore of Rapid7 reported on the blogger's findings, saying that "a researcher going by the name someLuser detailed a number of security flaws in the Ray Sharp DVR platform. These DVRs are often used for closed-circuit TV (CCTV) systems and security cameras. In addition to Ray Sharp, the exposures seem to affect rebranded DVR products," he said, and listed over 12 such names.

Fundamental to the problem in the identified DVR platform showing vulnerability is that it supports the Universal Plug and Play (UPnP) protocol. Many routers enable UPnP by default, exposing the vulnerable DVR to the Internet. The DVRs are automatically made visible to

external connections using the UPnP protocol. Rapid7 's Moore attributes the problem to design potentially leaving homes and businesses exposed "because of the way these things cut holes in the firewall."

Moore was able to identify some companies that seem to use the code. One of them, Zmodo, however, said it does not use faulty code and that it developed its own inhouse firmware with a substantially higher level of security, and has never been susceptible to the same intrusions as the firmware pegged as vulnerable. Other vendors may tackle the problem sooner than later too. Several vendors that had been listed reported that they were investigating the matter.

Meanwhile, the blogger someLuser suggested owners of affected DVRs temporarily disable UPNP on their routers. Rapid7 released a tool to help identify devices on its website.

More information: console-cowboys.blogspot.com/2 … -dvr-insecurity.html
www.forbes.com/sites/andygreen … to-hacker-hijacking/
community.rapid7.com/community … etrieval-remote-root