Software weaknesses can cause loss of lives in medical industry

Associated Press

OULU, Finland & SARATOGA, Calif.--(BUSINESS WIRE)--Jun 26, 2012-- Codenomicon, the leading vendor of proactive security testing software, has joined the Medical Device Innovation, Safety and Security Consortium (MDISS) to enhance the security in solutions and devices in the healthcare industry. Security test automation provided by Codenomicon will help the medical industry in building safety-critical systems.

"This cooperation helps the medical device industry to make their solutions even more reliable and to save lives in the long run," says Dr. Dale Nordenberg, Executive Director and Co-Founder of MDISS.

Codenomicon's Defensics test tool relies on fuzz testing, a technique where invalid or unexpected input is fed to the system under test to reveal potentially harmful software flaws. Attacks to medical devices can come from communication interfaces such as Bluetooth.

"A large percentage of medical devices are now connected to the outside world through wireless and fixed data-networks," says Jeff Walker from Codenomicon. "Until now, there hasn't been a focus on testing these systems thoroughly for threats or vulnerabilities," he continues.

The technique used by Codenomicon is particularly effective in finding previously unknown, so called zero-day vulnerabilities. Unknown vulnerabilities are a challenge to product security, since there are no patches available, no way to protect the system against attacks targeted to unknown vulnerabilities.

"The person receiving the treatment is placing their health on the line in case medical devices fail to work reliably or are vulnerable to malicious activities," says Kari Hytönen from Codenomicon. "The potential loss of life due to inappropriate security testing is negligence as the solutions are available to the industry." Codenomicon Unknown Vulnerability Management (UVM) helps organizations to locate zero-day vulnerabilities within their systems before they pose a threat, but also the methodology on how to remediate them.

For more information on Unknown Vulnerability Management, visit:http://www.codenomicon.com/unknown For more information on security of medical devices, visit:http://www.codenomicon.com/solutions/medical/ For more information on the Medical Device Innovation, Safety and Security (MDISS) consortium go to:http://www.mdiss.org For more information contact: -- Mr Jeff Walker, Codenomicon Business Development, Medical Systems Security Testing, jeff@codenomicon.com -- Mr Kari Hytönen, Codenomicon Manager of Security

Strategies and Standards, kari@codenomicon.com -- Dr Dale Nordenberg, MDISS Executive Director and Co-Founder, dalenordenberg@novasano.com About Codenomicon Ltd Codenomicon finds security vulnerabilities others can't find.

Companies rely on Codenomicon's solutions to discover zero-day vulnerabilities that cause Denial of Service (DoS) and data leakage if exploited by hackers -- the unknown vulnerabilities Advanced Persistent Threats (APTs) use to break into systems. Codenomicon's customers include Alcatel-Lucent, AT&T, Cisco Systems, Microsoft, Motorola, Google, Verizon, Nokia Siemens Networks, Huawei, and T-Systems.

Source URL (retrieved on *04/27/2015 - 10:19am*):
http://www.mdtmag.com/news/2012/06/software-weaknesses-can-cause-loss-lives-medical-industry