NEWS RELEASE

OSEHRA
900 N. Glebe Road
Arlington, VA 22203
Tel (571) 858-3061
www.OSEHRA.org

OSEHRA
Open Source Electronic Health Record Agent

FOR IMMEDIATE RELEASE
November 15, 2013

Contact: Maureen Markey 571-309-9483
markeym@osehra.org
Desereé Johnston 571-858-3181
johnstond@osehra.org

Power of Open Source Demonstrated by Successful Response to Electronic Health Record Vulnerability

Arlington, VA – Open source collaboration has tightened the security of one of the most widely used Electronic Health Record (EHR) systems in the world. In July 2013, Georgia Tech graduate student Doug Mackey evaluated the VistA (Veterans Health Information Systems and Technology Architecture) EHR for a term project on computer security. That project uncovered a significant security vulnerability, catalyzed a landmark collaboration between the U.S. Department of Veterans Affairs (VA) and the open source community, and created a textbook example of how the concept of open source can improve system security.

The collaborative response was led by the Open Source Electronic Health Record Agent (OSEHRA), a non-profit corporation founded to be the hub of open source EHR collaboration. "We're very proud of both the process and the outcome here," said Dr. Seong Ki Mun, CEO of OSEHRA. "A single interested individual found a vulnerability that impacted the entire community. Every VistA user can use the resulting patch to improve security for their patients. The level of cooperation among agencies, companies, and individuals was unprecedented, and demonstrates the real power of the open source community."

Mackey's original intent was to show the vulnerability of large critical infrastructure systems to attack by nation states and other organized threats. He chose VistA because of its wide deployment in VA hospitals and clinics and increasingly widespread use in the private sector. After obtaining an open source version of the VistA software, Mackey began a systematic examination of the code base and found what appeared to be a significant security hole in an obscure communications broker program. It appeared that, with some creative formatting, a message could be sent that enabled the sender to subsequently execute a wide variety of remote commands without authentication.

A team of OSEHRA staff and corporate members, including the VistA Expertise Network (VEN), DSS, Inc., Medsphere, iCare, and California's Oroville Hospital operated under non-disclosure as they developed a patch. VEN led the code development effort. A parallel effort was already underway at VA, and they soon added a representative to the OSEHRA team as well. The Indian Health Service, whose Resource and Patient Management System (RPMS) also appeared vulnerable, added their own representative to the team.

The VA patch focused on the immediate threat, while the OSEHRA patch included some additional features that resulted from community collaboration. VA decided not only to fast-track its own patch for distribution, but also to bring the OSEHRA open source version into VA as the next step of their process. Installations at VA and the IHS have received the VA patch, and the OSEHRA patch is publicly available for download at www.oeshra.org.

###

OSEHRA is a non-profit organization dedicated to accelerating innovation in electronic health record software and related technology. Founded in 2011, OSEHRA is a rapidly growing open source community with over 2,300 registered members representing 160+ industry, academic, and government organizations. OSEHRA supports an open, collaborative community of users, developers, and researchers engaged in advancing electronic health record software and related health information technology. OSEHRA hosts software repositories for applications such as the Department of Veterans Affairs' VistA electronic health record.