

8 May 2008

By: Traian Teglet, Technology News Editor



Wonderware is part of
Invenys Group
Invenys Process
Systems

[Wonderware SuiteLink's Denial of Reported Service Vulnerability](#)

The report was issued on Monday in a CoreLabs Advisory

Security researchers at Core Security Technologies have issued a warning statement on Monday according to which they found a rare vulnerability in Wonderware subsidiary's InTouch SuiteLink application. Wonderware, a business unit of Invenys, is a software manufacturer that offers solutions to business users in areas such as Production and Performance Management, Geographical SCADA and Supervisory HMI (Human-Machine Interface). Core Security found the vulnerability in Wonderware SuiteLink Service and it is said that the flaw allows the interference of an unauthenticated remote control that could shutdown the service. This means that a hacker could breach the SCADA (Supervisory Control And Data Acquisition) application by connecting to a SuiteLink service TCP port. The vulnerability hasn't been proven to allow remote code execution but according to Core Security, a potential scenario hasn't been excluded. According to the Security company, systems running WonderWare SuiteLink prior to version 2.0 Patch 01 are susceptible to the reported bug. While testing a system running WonderWare InTouch 8, Sebastian Muniz from the Exploit Writers Team, has discovered the above mentioned vulnerability. According to the American National Institute of Standards and Technology (NIST), the bug has been reported as being a high-risk one. Wonderware has made available to its registered customers a technical document addressing this issue. With consumer and business software applications this sort of breaches are somewhat common. Bugs involving SCADA applications aren't that frequent, but they can cause a lot of damage. There are a number of security companies that try to develop protective software applications for SCADA systems. According to Wonderware's website "one third of the world's plants run Wonderware software solutions.". A hacking attack that could make use of the discovered vulnerability will most certainly cause some serious damage on a worldwide scale. Wonderware customers still running systems using SuiteLink 2.0 Patch 01 should contact the company website for more information.