



Media statement

For further information:

Majella Nolan
Global Marketing Manager
Citect
Tel: + 61 412 587 711

Stephen Flannigan
Global Director CitectSCADA
Citect
Tel: +61 417 685 520

Security Update

Sydney, Australia [September 9, 2008] – Citect has been made aware of the publication of code that could be used to exploit a vulnerability that could cause a potential security breach if deliberately executed against a CitectSCADA system. This code targets a vulnerability in Citect Windows-based control systems for which a patch was released in June 2008.

Since the original publication of this vulnerability by Core Security Technologies, Citect has been working with its customers to encourage, and help them, to apply the patch. To date, no customers have reported security breaches.

While all customers should be applying reasonable network security measures, Citect encourages customers not running the patch to contact Citect support or visit the company's website and update their systems accordingly.

In the 21 year period over which Citect has been designing SCADA software, Citect has consistently recommended to its customers that they follow industry best practices in the development and implementation of control systems. In relation to security measures, Citect's position on SCADA and process control network security has remained unchanged – SCADA systems, like any business systems, must be protected from unauthorized access. They must be secured by robust protection including firewalls, intrusion detection systems and VPNs.

In addition to revised internal security handling processes, Citect remains committed to working closely with security agencies, customers and partners to ensure its software meets their security guidelines. Revised measures underway include, but are not limited to, an independent code audit, the provision of customer site review capabilities, a new security and safety knowledgebase and RSS feed. In addition, Citect will soon release a new version of CitectSCADA that applies further enhanced security measures to the software as part of the company's continued commitment to SCADA security.

"SCADA systems were originally designed and implemented before cyber security became the issue it is today, and so some SCADA systems are vulnerable when connected to the Internet," says Christopher Crowe, Citect's global CEO. "Citect is continuously striving to improve the security of its software and meet best-practice guidelines through the implementation of robust development and testing procedures."

For further information on this or any related security issue, please visit Citect's website or contact a local Citect representative.

About Citect

Citect is a global provider of industrial and facilities automation, real-time intelligence, and next generation manufacturing execution systems (MES). Leveraging open technologies, CitectSCADA, CitectFacilities and Ampla connect to multiple plant and business systems. Its products are complemented by Professional Services, Global Customer Support and Educational Services. Distributed in more than 80 countries worldwide, Citect solutions are installed in numerous industries: mining, metals, food and beverage, manufacturing, facilities, water/wastewater, oil and gas, power generation/distribution and pharmaceuticals. Citect has offices in Oceania, Africa, the Americas, Europe, India, Japan and Southeast Asia. For more information please visit www.citect.com.