

SCADA industry debates flaw disclosure

Robert Lemos, SecurityFocus 2006-06-16

The outing of a simple crash bug has caused public soul-searching in an industry that has historically been closed-mouthed about its vulnerabilities.

The flaw, in a particular vendor's implementation of the Inter-Control Center Communications Protocol (ICCP), could have allowed an attacker the ability to [crash a server](#). Yet, unlike corporate servers that handle groupware applications or Web sites, the vulnerable server software--from process-control application maker LiveData--monitors and controls real-time devices in electric power utilities and healthcare settings. The best known types of devices are supervisory control and data acquisition (SCADA) devices and distributed control system (DCS) devices.

A crash becomes a [more serious event](#) in those applications, said Dale Peterson, CEO of [Digital Bond](#), the infrastructure security firm that found the flaw.

"These are what you would consider, in the IT world, critical enterprise applications," Peterson said. "But the companies don't act like these are critical enterprise applications."

LiveData maintains that the flaw is a software bug, not a security vulnerability, pointing out that it only affects how the LiveData ICCP Server handles a non-secure implementation of the communications protocol--typically used only in environments not connected to a public network.

"In general SCADA networks are run as very private networks," said Jeff Robbins, CEO of LiveData. "You cannot harness an army of public zombie servers and attack them, because they are not accessible."

The incident has touched off a heated debate among a small collection of vulnerability researchers, critical infrastructure security experts and the typically staid real-time process control systems industry. The controversy mirrors the long-standing dispute between independent researchers and software vendors over disclosing vulnerabilities in enterprise and consumer applications. In that industry, researchers have taken [Apple](#), [Oracle](#), [Cisco](#) and [Microsoft](#) to task at various times over the last year for the perception that the companies were not [responding adequately](#) to reports of flaws in their software products.

Last week at the Process Control System Forum (PCSF), a conference on infrastructure management systems funded by the U.S. Department of Homeland Security, a similar debate played itself out. Perhaps three dozen industry representatives and security researchers met during a breakout session to hash out the issues involving disclosure. The tone became, at times, contentious, said Matt Franz, the moderator at conference panel on the topic and a SCADA security researcher with Digital Bond.

"The vendors were sticking together saying that (researchers) didn't need to be involved with SCADA flaws," he said. "'It puts people and infrastructure in danger,' they said."

Moreover, many vendors did not appreciate the involvement of the U.S. Computer Emergency Readiness Team (US-CERT), the nation's response group tasked with managing the process of vulnerability remediation for critical infrastructure, Franz said.

The LiveData flaw was the first flaw in SCADA systems handled by US-CERT and the CERT Coordination Center, the group that manages the national agency. While valuable as a learning experience, the entrance of a third party into the disclosure of a flaw in an infrastructure system brought up more questions than answers. At the PCSF session, many vendors voiced concerns over involving a third party.

"I did not come away with a feeling that any issues were settled," said Art Manion, Internet security analyst for the CERT Coordination Center and a participant in the discussion at the conference.

The debate over how disclosure should be handled underscores both the intense focus on SCADA and DCS systems as potential targets of cyberattacks and the position of many companies in the real-time process control systems industry that vulnerabilities in such systems require special treatment.

"In security circles, it is widely discredited that you can secure something though obscurity--yet SCADA systems are really obscure," LiveData's Robbins said. "That is not a statement of a principle of security and doesn't rationalize anything, but is a fact."

Even SCADA security specialists agree that obscurity can raise the hurdle enough to keep most online attackers from jumping into SCADA systems.

"There are some legacy systems out there running plants that are more secure than many latest and greatest systems, because they are not connected to the Internet or they are using obscure standards," said Ernest Rakaczky, program director for process control systems at infrastructure firm Invensys.

That's true--at least to an extent, said CERT Coordination Center's Manion.

"The information on these systems can be found by a determined attacker," Manion said. "Part of our outreach is to show that people can find out about these things and find vulnerabilities."

Consultants who have done penetration testing and security audits of real-time process control systems tell grim stories about the lack of security in the systems. Data is transferred with no encryption using protocols, such as Telnet and FTP, that are being phased out in other industries; many firewalls have ports opened to any traffic; and, many workstations still run Windows NT, said Jonathan Pollet, vice president and founder of PlantData Technologies, a division of infrastructure security company Verano.

"The guys who are setting up these systems are not security professionals," he said. "And many of the systems that are running SCADA applications were not designed to be secure--it's a hacker's playground."

For between 5 and 10 percent of the networks audited by PlantData, a single ping attack or a data flood aimed at a SCADA system could shut down most of the managed devices, Pollet said.

Yet, security researchers acknowledge that the software that monitors, manages and runs the variety of manufacturing and infrastructure control systems is indeed different. While researchers can hold the threat of public disclosure over the heads of an uncooperative software maker in the enterprise application arena, publicly outing a flaw in a SCADA or DCS system has larger ramifications, Pollet said.

"You have to be careful disclosing these issues to the public when the vendors seem uninterested in talking about the problem, because these systems cannot be patched overnight and the information could prove devastating in the wrong hands," he said.

Moreover, software vendors and infrastructure operators legitimately need more time because most of the industry's legacy systems were not created to be easily updated. And, to be fair, LiveData's response to the first SCADA vulnerability handled by a third party--about 3 to 6 months for a fix and less than 9 months for notification--is in line with the response from many enterprise and commercial software makers. Not bad for an industry that has not had a history of third-party vulnerability disclosure, said

Digital Bond's Franz.

"The idea that someone outside their customer base would have access to their product to find vulnerabilities is strange to them," said Franz, who created an [interest group](#) within the Process Control Systems Forum to hash out the issues.

Security researchers are not the only ones applying pressure to software developers in the SCADA and DCS industry. The software maker's customers--infrastructure owners and operators--are starting to demand proof of security audits, especially in the power industry where companies are required by a recent law to adhere to the Critical Infrastructure Protection (CIP) guidelines published by the North American Electric Reliability Council (NERC).

"The difference that a few months has made is absolutely incredible," said Lori Dustin, vice president of marketing and services for infrastructure security company Verano. "The people I'm meeting with now have a copy of the NERC documents in their hands."

While many in the real-time process control industry might not agree, Invensys's Rakaczky stresses that allowing US-CERT to bring other industries' vulnerability reporting practices to the bear on infrastructure issues should help reduce communications problems and increase trust.

"People will respond faster than if some random white hat calls them up out of the blue," he said.

But, while vendors work with US-CERT and focus on improving product security, infrastructure owners need to move more quickly to prevent unauthorized access to their systems from the Internet and implement more strict auditing, Rakaczky said.

"Right now, we need perimeter protection," he said. "We need to stop the wound from bleeding before we can heal it."

[Privacy Statement](#)

Copyright 2006, SecurityFocus