Home / Security / News

NEWS

Computer Threat for Industrial Systems Now More Serious

By Robert McMillan

PCWorld | SEP 10, 2008 12:20 AM PDT

A security researcher has published code that could be used to take control of computers used to manage industrial machinery, potentially giving hackers a back door into utility companies, water plants and even oil and gas refineries.

The software was published late Friday night by Kevin Finisterre, a researcher who said he wants to raise awareness of the vulnerabilities in these systems, problems that he said are often downplayed by software vendors. "These vendors are not being held responsible for the software that they're producing," said Finisterre, who is head of research with security testing firm Netragard. "They're telling their customers that there is no problem, meanwhile this software is running critical infrastructure."

00:03 / 24:06

Finisterre released his attack code as a software module for Metasploit, a widely used hacking tool. By integrating it with Metasploit, Finisterre has made his code much easier to use, security experts said. "Integrating the exploit with Metasploit gives a broad spectrum of people access to the attack," said Seth Bromberger, manager of information security at PG&E. "Now all it takes is downloading Metasploit and you can launch the attack."

The code exploits a flaw in Citect's CitectSCADA software that was originally discovered by Core Security Technologies and made public in June. Citect released a patch for the bug when it was first disclosed, and the software vendor has said that the issue poses a risk only to companies that connect their systems directly to the Internet without firewall protection, something that would never be done intentionally. A victim would have to also enable a particular database feature within the CitectSCADA product for the attack to work.

These types of industrial SCADA (supervisory control and data acquisition) process control products have traditionally been hard to obtain and analyze, making it difficult for hackers to probe them for security bugs, but in recent years more and more SCADA systems have been built on top of well-known operating systems like Windows or Linux making them both cheaper and easier to hack.

IT security experts are used to patching systems quickly and often, but industrial computer systems are not like PCs. Because a downtime with a water plant or power system can lead to catastrophe, engineers can be reluctant to make software changes or even bring the computers off-line for patching.

This difference has led to disagreements between IT professionals like Finisterre, who see security vulnerabilities being downplayed, and industry engineers charged with keeping these systems running. "We're having a little bit of a culture clash going on right now between the process control engineers and the IT folks,"

Citect said that it had not heard of any customers who had been hacked because of this flaw. But the company is planning to soon release a new version of CitectSCADA with new security features, in a statement, (pdf) released Tuesday.

That release will come none too soon, as Finisterre believes that there are other, similar, coding mistakes in the CitectSCADA software.

And while SCADA systems may be separated from other computer networks within plants, they can still be breached. For example, in early 2003, a contractor reportedly infected the Davis-Besse nuclear power plant with the SQL Slammer worm.

"A lot of the people who run these systems feel that they're not bound by the same rules as traditional IT," Finisterre said. "Their industry is not very familiar with hacking and hackers in general."

Note: When you purchase something after clicking links in our articles, we may earn a small commission. Read our affiliate link policy for more details.

Related: Security

PCWorld helps you navigate the PC ecosystem to find the products you want and the advice you need to get the job done.

POLICIES

ABOUT