

Zero Day

Ryan Naraine, Dancho Danchev, Nate McFeters

June 12th, 2008

Hacking SCADA for terrorism and destruction

Posted by Nathan McFeters @ 12:26 am

SCADA scares me, and I've seen enough things on the Internet to be desensitized to many things, but attacks against SCADA threaten our national security in a very real and topical way by attacking power grids, water treatment plants, nuclear plants, etc. Hacking networks that SCADA devices reside on and using that access to interact with the SCADA system is nothing really new, it's been covered in the media quite a bit... including the infamous Idaho National Labs research video which was ridiculously disclosed to CNN by our very own Department of Homeland Security director, who should've been keeping this to himself and creating a serious plan to address these issues, rather than giving terrorists something to salivate over. If you haven't seen this video, I suggest you have a look as you'll see a generator connected to a SCADA device nearly blow up when sent an Internet based attack.



What we haven't seen a ton of are specific attacks against SCADA devices and protocols. Why? SCADA devices can be expensive, or impossible to setup and replicate for those doing vulnerability research (with Idaho National Labs maybe being one of the examples where this isn't an issue) and clients typically would be well advised to NOT assess the protocols on their direct production systems (seems obvious, but you never know). So what's new about my article today? Well, our good friends at Core Security Technologies in Boston released an advisory today about a buffer overflow attack in a specific SCADA product.

Read more by clicking the more link below.

In an exclusive interview with the Associated Press, Core Security Technologies and the article author, Jordan Robertson, comment on the advisory:

Citect Pty. Ltd., which makes the program called CitectSCADA, patched the hole last week, five months after Core Security first notified Citect of the problem.

But the vulnerability could have counterparts in other so-called supervisory control and data acquisition, or SCADA, systems. And it's not clear whether all Citect clients have installed the patch.

First off, not to call CitectSCADA out, cause I'd imagine this is not something they deal with all of the time, but five months is a long time to have an issue of this magnitude in such critical pieces of our nation's infrastructure. Again, I don't fault Citect on that, I'm simply stating the prospect is scary. Vulnerabilities in the software that manages SCADA devices, the protocols associated

with that interaction, and other areas of SCADA technologies have been talked about for quite some time as security concerns. In fact, not that long ago several people on Full Disclosure's mailing list were discussing direct research being performed on specific SCADA devices which led to some Denial of Service vulnerabilities.

Second, the fact that Citect and other SCADA companies may not have considered things like patch management (by the way, I'm only theorizing here, I don't pretend to know how Citect handles their patch management process, but it would seem likely to be something a lot of SCADA companies have not considered) is very concerning as this simple yet devastating issue could be around for a lot longer. The Associated Press article goes on to say:

The Citect vulnerability is of a common type. Called a "buffer overflow," it allows a hacker to gain control of a program by sending a computer too much data.

"It's not a very elaborate problem," Ivan Arce, Core Security's chief technology officer, said in an interview. "If we found this thing — and this was not that hard — it would be easy for someone else to do it."

It's a great point made by Ivan, which I think a lot of people miss when thinking about security research. If the good guys can find it, so can the bad, and it's irresponsible to think they haven't or aren't looking. The article also describes how this might be attacked as follows:

For an attack involving the vulnerability that Core Security revealed Wednesday to occur, the target network would have to be connected to the Internet. That goes against industry policy but does happen when companies have lax security measures, such as connecting control systems' computers and computers with Internet access to the same routers.

A rogue employee could also access the system internally.

Ok, so hang on here, I tend to disagree with this a bit. So, when the term Internet is used in this context, I'm going to assume that the author of the article means the externally accessible Internet, where as the internal only accessible piece of the Internet is going to be called a company's Intranet. This is pretty standard terminology, but we need to point it out to be on the same page. Really, the statement that the target network would have to be connected to the Internet is actually untrue. The article mentions rogue employees, and that covers another threat, but these are what I see as the actual threats:

1. Rogue employees that can access the SCADA network from their corporate Intranet
2. Third-party contractors given guest access to any network in a corporation, as trust relationships between domains can be leveraged to gain access to other networks
3. Third-party or employees given VPN access to the corporate Intranet, as depending upon the implementation of VPN access, this could be vulnerable to attack... especially consider web application VPN portals that might be vulnerable to cross-site scripting allowing me to steal a valid VPN user's session giving me the capability to load the VPN connection/software
4. The Internet (hopefully a SCADA devices is not corrected direct to the Internet)
5. Any firewall bypassing attacks that might be useful leading to vulnerability linkage getting us to this internal SCADA network. This one is really important. There's a lot of web application based attacks
 1. See Protocol Handler Abuse, research published by myself, Billy Rios, and Rob Carter
 2. See anti-DNS pinning attacks including research by myself, Billy Rios, Rob Carter, Dan Kaminsky, Kanatoko, Martin Johns, etc.
 3. These types of attacks may allow an attacker to deploy serious attacks to a high traffic

web application, using cross-site scripting as the deployment vector. Once a user has been compromised by the cross-site scripting attack, the attacker can use anti-DNS pinning to use the victim's browser to interact with internally accessible resources to the network the victim is on, or use protocol handling attacks to try to compromise the underlying operating system of the victim's machine, thus giving the attacker a foothold into the internal network.

4. For even more in application/browser flaws that turn into extremely serious issues, see my talk at Black Hat Vegas '08 this year with Rob Carter, John Heasman, and Billy Rios... teaser here.

These web application attacks that allow crossing over the boundary put in place by the firewall are extremely concerning when you consider vulnerability linkage which may ultimately lead to the compromise of a SCADA device. Consider the impact of a successful compromise of a SCADA device, which the original AP article so accurately described:

Security experts say the finding highlights the possibility that hackers could cut the power to entire cities, poison a water supply by disrupting water treatment equipment, or cause a nuclear power plant to malfunction by attacking the utility's controls.

Eeek... the article also mentions that Citect suggests that companies using SCADA devices segregate the devices from the Internet... well, that's certainly a great recommendation, but they go on to mention proper firewall configuration, etc. Again, this is a great step, but I think it is very important to underscore that simple firewall rules to the outside world of the Internet only eliminate a piece of the attack space. As I mentioned, internal employees, third-parties given access, and compromise of users of the companies network may again put the SCADA device at risk.

So then, we need to ask ourselves... is the threat real? Hopefully you saw the video I linked to above, but if that wasn't enough to get your concern level up, the CIA reported that a power outage in several cities outside of the United States was actually caused by hackers who had demanded money or threatened to turn out the lights. Another example that strikes much closer to home is something I think a lot of us will remember, when the lights went out on a large portion of the eastern seaboard. National Journal Magazine conducted interviews with government officials who believed the power outages to have actually been caused by Chinese hackers:

One prominent expert told *National Journal* he believes that China's People's Liberation Army played a role in the power outages. Tim Bennett, the former president of the Cyber Security Industry Alliance, a leading trade group, said that U.S. intelligence officials have told him that the PLA in 2003 gained access to a network that controlled electric power systems serving the northeastern United States. **The intelligence officials said that forensic analysis had confirmed the source, Bennett said. "They said that, with confidence, it had been traced back to the PLA." These officials believe that the intrusion may have precipitated the largest blackout in North American history, which occurred in August of that year. A 9,300-square-mile area, touching Michigan, Ohio, New York, and parts of Canada, lost power; an estimated 50 million people were affected.**

So in conclusion, the threat is real. If you are a vendor of SCADA devices, get your products assessed. If you are a company using SCADA devices, get an Internet/Intranet/Extranet assessment done to try to determine how well you've segregated these devices from the rest of the network and make appropriate corrections based upon those results.

-Nate



Nathan McFeters is a Senior Security Advisor for Ernst & Young's Advanced Security Center in Chicago. The views and opinions expressed in this article are his own and do not represent the views and opinions of Ernst & Young Advanced Security Center or Ernst & Young, LLP. Nathan has performed web application, deep source code, Internet, Intranet, wireless, dial-up, and social engineering engagements for numerous clients in the Fortune 500 during his career at Ernst & Young and has spoken at a number of prestigious conferences, including Black Hat, DEFCON, ToorCon, and Hack in the Box. He can be found at his Pwn* blog and XS-Sniper, a blog with Billy Rios. See his full profile and disclosure of his industry affiliations.

Copyright © 2008 CNET Networks, Inc. All Rights Reserved. [Privacy Policy](#) | [Terms of Use](#)