

Hole Found in Protocol Handling Vital National Infrastructure

Systems that control dams, oil refineries, railroads and nuclear power plants have a vulnerability that could cause a system takeover, according to a recent research report.

Researchers on March 21 announced that the systems which control dams, oil refineries, railroads and nuclear power plants have a vulnerability that could be used to cause a denial of service or a system takeover.

The flaw, reported by Neutralbit, is the first remotely exploitable SCADA security vulnerability, according to the security services provider. SCADA (supervisory control and data acquisition) is a large-scale, distributed measurement and control system used to monitor or control chemical or transport processes in municipal water supply systems, to control electric power generation, transmission and distribution, gas and oil pipelines and other distributed processes. Wikipedia has a schematic of SCADA [here](#).

Neutralbit identified the vulnerability in NETxAutomation NETxEIB OPC (OLE for Process Control) Server. OPC is a Microsoft Windows standard for easily writing GUI applications for SCADA. It's used for interconnecting process control applications running on Microsoft platforms. OPC servers are often used in control systems to consolidate field and network device information.

Neutralbit reports that the flaw is caused by improper validation of server handles, which could be exploited by an attacker with physical or remote access to the OPC interface to crash an affected application or potentially compromise a vulnerable server. Neutralbit has also recently published [five vulnerabilities](#) having to do with OPC.

This isn't the first time that this vital bit of national infrastructure has gotten a black eye. Errata President Robert Graham published a scathing report last year titled "SCADA Security and Terrorism: We're Not Crying Wolf." In that report and in his more recent blog, he called SCADA "completely open to attack, especially OPC."

Graham described the OPC Windows applications as being used to translate between Windows primitives such as MS-RPC/DCOM to back-end protocols that do the actual monitoring and controlling of switches, valves, pressure gauges, thermometers, and so forth.

"These backend protocols are often based upon standards that pre-date Windows," Graham wrote in his blog. "They are horribly insecure because few people in the SCADA industry know what a 'buffer-overflow' is."

Graham said that it took him all of five minutes to find a remotely exploitable bug when he downloaded sample implementations from the OPC Foundation a few years ago.

Graham said that the real problem isn't vulnerabilities but the fact that OPC installations are normally run without authentication such as a username and password. " - That - means a hacker can control them without having to mess around with things like buffer overflows," he wrote.

If proper authentication and encryption are in fact enabled, a hacker can't actually remotely exploit OPC installations without first logging on, Graham said. This is the case with the vulnerability reported by Neutralbit, he said: "It's only exploitable if the user has login privileges."

In fact, Graham said, he doesn't believe that many SCADA organizations will take this recent vulnerability

warning seriously because they know that since their systems are already wide open to attack, patching them against this bug won't stop a hacker.

"That would be wrong," Graham said. "First, there is the possibility of - a - worm exploiting these bugs. Second, at some point the SCADA industry is going to have to catch up with the rest of the world with regards to securing their products.

"Neutralbit has done an excellent job of explaining to you potential problems with OPC, but they've also explained them to hackers and cyber-terrorists. Any kid who wants to prove he's a vulnerability hunter now knows he can go onto eBay, get some cheap OPC products, find vulnerabilities in them, and announce them to the world."

Graham says there's a "good chance that many more OPC vulnerabilities will be announced and/or exploited in the next couple years."

NETxAutomation has addressed the flaw by releasing version 3.0.1300 of the NETxEIB OPC Server. The company has also released a patch for NETxEIB OPC Server version 3.0. US-Cert recommends restricting remote access to the server to only trusted hosts by using firewalls or only connecting them to private networks, until a fixed version of the server can be deployed.

According to its Web site , Neutralbit has issued the vulnerability disclosure in collaboration with US-CERT - whose advisory is here - and the affected vendors.

Copyright 2007 by Ziff Davis Media, Distributed by United Press International

This document is subject to copyright. Apart from any fair dealing for the purpose of private study, research, no part may be reproduced without the written permission. The content is provided for information purposes only.