



>ONLINE SHOPPING AT WORK

Original URL: http://www.theregister.co.uk/2008/09/25/abb_critical_bug/

World's electrical grids open to attack

Scads of SCADA bugs

By [Dan Goodin in San Francisco](#)

Posted in [Security](#), 25th September 2008 18:03 GMT

A serious vulnerability has been found in yet another computerized control system that runs some of the world's most critical infrastructure, this time in a product sold by a vendor known as the ABB Group.

According to researchers from C4 - a firm specializing in the security of so-called SCADA, or Supervisory Control And Data Acquisition, systems - ABB's Process Communication Unit (PCU) 400 suffers from a critical buffer overflow bug.

"The vulnerability was exploited by C4 to verify it can be used for arbitrary code execution by an unauthorized attacker," researcher Idan Ofrat wrote in [this advisory](#) (<http://www.securityfocus.com/archive/1/496739>) published on Thursday. "In addition, an attacker can use his control over the FEP server to insert a generic electric grid malware...in order to cause harm to the grid."

The vulnerable software controls critical national infrastructure, including electrical grids. The vulnerability affects versions 4.4, 4.5, and 4.6, and possibly others, the C4 advisory warns.

ABB has issued a patch for the bug.

The advisory comes as concern mounts about the safety of software used to run gasoline refineries, manufacturing plants and other industrial facilities. In June, a now-patched vulnerability in CitectSCADA potentially exposed plants' critical operations to outsiders or disgruntled employees. Law makers on [both sides](#) (http://www.theregister.co.uk/2008/08/26/uk_minister_grid_hacker_warning/) of [the Atlantic](#) (http://www.theregister.co.uk/2008/05/22/electrical_grid_vulnerable/) have warned that lax security may make critical infrastructure vulnerable to saboteurs or terrorists.

C4 is no stranger to security in SCADA systems. In January, it warned of vulnerabilities in two products made by Ge Fanuc. One of them resided in Ge Fanuc's [Cimplicity product](#) (<http://www.securityfocus.com/archive/1/487076>), and the other affected the company's Proficy Information Portal 2.6. Both appear to have have been patched. ®

Related stories

[Citect yanks 'misleading' SCADA bug advisory](#) (19 September 2008)

http://www.theregister.co.uk/2008/09/19/scada_advisory_pulled/

[Gas refineries at Defcon 1 as SCADA exploit goes wild](http://www.theregister.co.uk/2008/09/08/scada_exploit_released/) (8 September 2008)

http://www.theregister.co.uk/2008/09/08/scada_exploit_released/

[Minister warns of national grid hack threat](http://www.theregister.co.uk/2008/08/26/uk_minister_grid_hacker_warning/) (26 August 2008)

http://www.theregister.co.uk/2008/08/26/uk_minister_grid_hacker_warning/

[SCADA security bug exposes world's critical infrastructure](http://www.theregister.co.uk/2008/06/12/scada_vuln_discovered/) (12 June 2008)

http://www.theregister.co.uk/2008/06/12/scada_vuln_discovered/

[Electrical grid overlords take drubbing over cyber attack vulnerability](http://www.theregister.co.uk/2008/05/22/electrical_grid_vulnerable/) (22 May 2008)

http://www.theregister.co.uk/2008/05/22/electrical_grid_vulnerable/

[Rare SCADA bug poses power plant risk](http://www.theregister.co.uk/2008/05/08/scada_vuln/) (8 May 2008)

http://www.theregister.co.uk/2008/05/08/scada_vuln/

[CIA claims crackers took out power grids](http://www.theregister.co.uk/2008/01/21/scada_threat_warning/) (21 January 2008)

http://www.theregister.co.uk/2008/01/21/scada_threat_warning/

[Electrical supe charged with damaging California canal system](http://www.theregister.co.uk/2007/11/30/canal_system_hack/) (30 November 2007)

http://www.theregister.co.uk/2007/11/30/canal_system_hack/

['Data storm' blamed for nuclear plant shutdown](http://www.theregister.co.uk/2007/05/21/alabama_nuclear_plant_shutdown/) (21 May 2007)

http://www.theregister.co.uk/2007/05/21/alabama_nuclear_plant_shutdown/

[SCADA system makers urged to tighten security](http://www.theregister.co.uk/2006/07/28/scada_security_push/) (28 July 2006)

http://www.theregister.co.uk/2006/07/28/scada_security_push/

[Sluggish movement on power grid cyber security](http://www.theregister.co.uk/2004/08/16/power_grid_cybersecurity/) (16 August 2004)

http://www.theregister.co.uk/2004/08/16/power_grid_cybersecurity/

© Copyright 1998–2008