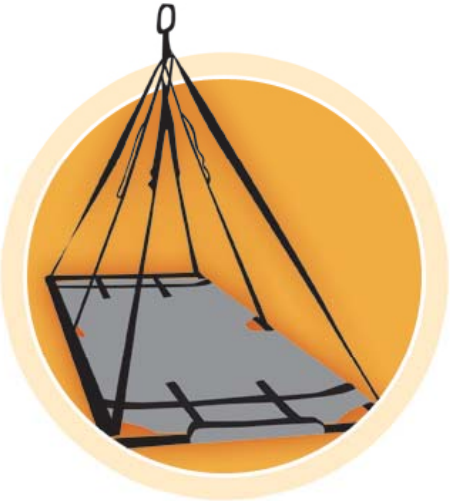

~~Responsible Disclosure~~
Effective Disclosure

Dale Peterson, Digital Bond, Inc.

peterson@digitalbond.com

digital bond

SECURING THE CRITICAL INFRASTRUCTURE

Image by
ThisParticularGreg

Image by
bocek.kevin

Image by Lisa Brewster

Image by lampertron

~~Responsible Disclosure~~

Effective Disclosure

OSIsoft

invensys™
Operations Management

ABB

Schneider Electric

SIEMENS

EMERSON™
Process Management

ALSTOM | GRID

Honest Forthright

Do these problems also affect other families of controllers like S7-300 and S7-400?

The S7-300 and S7-400 controllers are not affected by the denial-of-service scenario, so there is no need for any firmware update with these controllers in this regard.

Siemens site, June 2011

Image by cliff1066

Honest Forthright

"All vulnerabilities exploited by Stuxnet have been removed."

Ralf-Michael Franke, Siemens CEO for Industrial Automation Systems at Hannover Fair in April 2011

Image by cliff1066

Honest Forthright Clear

Image by pmschlenker

Specifically, it can result in RSLogix 5000 being unable to publish information to FactoryTalk Diagnostics and FactoryTalk AssetCentre. Additionally, exploitation can lead to a potential for a DoS and Denial of View (DoV) condition to other affected FactoryTalk-branded software. Such DoS and DoV conditions can prevent affected software from establishing communication or maintaining information exchange with servers and other control system devices.

Impact from ICSA-11-173-01

Successful exploitation of this vulnerability allows an attacker access to diagnostic information without proper authentication.

Impact from ICSA-11-231-01

Impact to individual organizations depends on many factors that are unique to each organization.

ICS-CERT recommends that organizations evaluate the impact of this vulnerability based on their operational environment, architecture, and product implementation.

From ICS-ALERT-11-245-01

The public disclosure indicates that these vulnerabilities are remotely exploitable… Specifically, the two disclosed vulnerabilities are:

- A format string vulnerability
- A memory corruption vulnerability

From ICS-ALERT-11-255-01

Currently, the exploit code allows an attacker the ability to bind a shell. Simple modifications of this exploit code could result in additional impacts to systems running affected versions of the products.

Image by Victor Svensson

RA RSLogix vuln

- Identified Sept 13
- Committed date on Sept 30
- Fix by Oct 14; actual Oct 5

Beresford Siemens S7 Vulns

- Identified May/June/July
- Quick fix for some
- No dates for the rest

Silent Fix

MITIGATION

Affected CPUs and firmware versions are listed in the table below.

PLC Name	Affected Version	Fixed In	Date Fixed
CPU315(including F)-2PN/DP	V2.6 and previous	V3.1	10/2009
CPU317(including F)-2PN/DP	V2.6 and previous	V3.1	10/2009
CPU319(including F)-3PN/DP	V2.7 and previous	V2.8	06/2009
IM151-8(including F) PN/DP CPU	V2.7	V3.2	08/2010
IM154-8 PN/DP CPU	V2.5	V3.2	08/2010
S7-400 – All Models	Not Affected		

Image by Iain Farrell

Image by Brooks Elliott

Effective Disclosure

1. Honest
2. Forthright
3. Clear
4. Impact – Vendor for End User, CERT for Public
5. Timeline