# Important security notification – vulnerability within Vijeo Citect / CitectSCADA / PowerLogic SCADA

16 July, 2013

Schneider Electric® has become aware of a possible vulnerability related to XML External Entity (XXE) processing in the following products:

- Vijeo Citect$^{TM}$
- CitectSCADA$^{TM}$
- PowerLogic SCADA$^{TM}$

## The Vulnerability Identified

The vulnerability could lead to the disclosure of confidential information by allowing access to local resources (files and internal resources) or have other system impacts (e.g. Denial of Service).

This vulnerability was discovered during cyber security research both by an external researcher and by Schneider Electric internal investigations. There is no evidence that this vulnerability has been exploited. This vulnerability would require network access to the target application.

Schneider Electric takes these vulnerabilities very seriously and we have devoted resources to immediately investigate and address these issues. We believe it is critical to consider the whole picture, including safety, security and reliability. Any patches/solutions/mitigations we release will be carefully tested allowing them to be deployed in a safe and secure manner.

## Details on Products Affected

- Vijeo Citect$^{TM}$ v7.20 and all previous versions
- CitectSCADA$^{TM}$ v7.20 and all previous versions
- PowerLogic SCADA$^{TM}$ v7.20 and all previous versions

## Recommendation

Schneider Electric has developed a patch which addresses the above vulnerability. These patches are available for all products affected.

Vijeo Citect:

- Version 7.20 of Vijeo Citect - http://www.citect.schneider-electric.com/vjc-HF720SP459363
- Version 7.10 of  Vijeo Citect - http://www.citect.schneider-electric.com/vjc-HF710SP459437

CitectSCADA:

- Version 7.20 of CitectSCADA - http://www.citect.schneider-electric.com/cs-HF720SP459363
- Version 7.10 of CitectSCADA - http://www.citect.schneider-electric.com/cs-HF710SP459437

PowerLogic SCADA:

- Version 7.20 of Power Logic SCADA Service Release 1- https://schneider-electric.box.com/pls720sr1

- Version 7.10 of Power Logic SCADA Service Release 4, https://schneider-electric.box.com/pls710sr4

**Schneider Electric recommends ALL customers using the above listed software packages to download and apply the relevant patch.**

## Acknowledgments

Schneider Electric wishes to thank the following people for working with us to help protect our customers:

- Timur Yunusov, Alexey Osipov and Ilya Karpov of Positive Technologies for reporting the vulnerability.

## Support

Vijeo Citect & CitectSCADA customers please contact the SCADA & MES Software Global Support Center located here:

http://www.citect.schneider-electric.com/contact-support

PowerLogic SCADA customers  please contact your local country support organization at:

http://www.schneider-electric.com/sites/corporate/en/support/operations/local-operations/local-operations.page

## CVSS Scoring

CVSS scores are a standard way of ranking vulnerabilities and are provided for reference, they should be adapted by individual users as required.

Base CVSS Score: 6.9 (AV:L/AC:M/Au:N/C:C/I:C/A:C)

## Frequently Asked Questions

**1) I am using an older release of the software discussed in this security notification. What should I do?**

**Vijeo Citect / CitectSCADA Products:**

The affected software listed in this notification has been tested to determine which releases are affected. Other releases are past their active support life cycle.

It should be a priority for customers who have older releases of the software to migrate to supported releases to prevent potential exposure to vulnerabilities. To determine the support lifecycle for your software release, please visit the appropriate link on the product support lifecycle page on the support website accessible at

http://www.citect.schneider-electric.com/index.php?option=com_content&view=article&id=873&Itemid=632

**PowerLogic SCADA Products:**

All versions of PowerLogic SCADA continue to be supported. The fixes provided for these versions should be applied to your PowerLogic SCADA system

**2) What should customers do if they install the fix, and then re-install the product?**
Customers should first uninstall the fix, re-install\repair the affected product(s) and then reinstall the fix.

### RSS Feed

If you would like to be notified of any future security issues of interest please register for the RSS feed on our Security Notification areas:

Schneider Electric CyberSecurity Notifications (All Products):
http://www2.schneider-electric.com/sites/corporate/en/support/cybersecurity/cybersecurity.page

Vijeo Citect / CitectSCADA / CitectHistorian / Vijeo Historian / Ampla / CitectFacilities Products:
Access Controlled Proactive Notifications:
http://www.citect.schneider-electric.com/proactive-safety-security
Public Notifications:
http://www.citect.schneider-electric.com/safety-security

## Legal

### Disclaimer

Schneider Electric is broadly distributing this Security Notification in order to bring to the attention of users of the affected Schneider Electric products the important security information contained in this Notification. Schneider Electric recommends that all users determine the applicability of this information to their individual situations and take appropriate action. Schneider Electric does not warrant that this information is necessarily accurate or complete for all user situations and, consequently, Schneider Electric will not be responsible for any damages resulting from user's use or disregard of the information provided in this notification. To the extent permitted by law, Schneider Electric disclaims all warranties, either express or implied, including the warranties of merchantability and fitness for a particular purpose, title and non-infringement.