Important security notification – Cumulative update for SCADA Expert Vijeo Citect / CitectSCADA / PowerSCADA Expert

SEVD 2014-024-02

24th Jan, 2014

Schneider Electric® has become aware of a possible security issue. The issues are:

- Security issue: Vulnerability related to an unhandled exception

The Security Vulnerability Identified

The vulnerability could cause a Denial of Service on the Server of the products listed below. To exploit this vulnerability an attacker must send a specially crafted packet to any of the Server processes.

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.

Products affected:

- StruxureWare SCADA Expert Vijeo Citect™ v7.40
- Vijeo Citect™ v7.20 to v7.30SP1
- CitectSCADA™ v7.20 to v7.30SP1
- StruxureWare PowerSCADA Expert™ v7.30 to v7.30SR1
- PowerLogic SCADA™ v7.20 to v7.20SR1

Note: Older versions of the products listed above are not affected by this vulnerability.

Recommendation

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

- SCADA Expert Vijeo Citect v7.40 - http://www.citect.schneider-electric.com/se-vjc-HF740RTM607771
- Vijeo Citect v7.30 SP1 - http://www.citect.schneider-electric.com/vc-HF730SP1607751
- Vijeo Citect v7.20 SP4 - http://www.citect.schneider-electric.com/vc-HF720SP4607691
- CitectSCADA v7.40 - http://www.citect.schneider-electric.com/cs-HF740RTM607771
- CitectSCADA v7.30 SP1 - http://www.citect.schneider-electric.com/cs-HF730SP1607751
- CitectSCADA v7.20 SP4 - http://www.citect.schneider-electric.com/cs-HF720SP4607691
- PowerSCADA Expert v7.30 SR1 - http://www.citect.schneider-electric.com/pse-HF730SP1608004
- PowerLogic SCADA v7.20 SR1 - http://www.citect.schneider-electric.com/pls-HF720SP460803

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

Schneider Electric takes these security and safety issues 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 tested to support both a safe and secure deployment.

Acknowledgments

Schneider Electric wishes to thank Carsten Eiram of Risk Based Security for reporting the security vulnerability and for working with us to help protect our customers

Support

If you are unsure of whether you could be affected by this security vulnerability or safety issue, or if you have any questions on this subject please contact our support centers:

If you are a SCADA Expert Vijeo Citect or CitectSCADA customer please contact the SCADA & MES Software Global Support Centre on: http://www.citect.schneider-electric.com/contact-support

If you are a PowerSCADA Expert or PowerLogic SCADA customer please contact your local country support organization on: http://www2.schneider-electric.com/sites/corporate/en/support/support.page

Or

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: 7.8 (AV:N/AC:L/Au:N/C:N/I:N/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 have been tested to determine which releases are imapcted. 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 Support Lifecycles page on the SCADA & MES Global Support website accessible at

http://www.citect.schneider-electric.com/about-support/support-lifecycle

PowerSCADA Expert / 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. To determine the support lifecycle for your software release, please visit https://powersolutionscommunity.schneider-electric.com/docs/DOC-1407

2)Does this patch need a service pack to be installed?

Customers should first install the latest service pack for their associated version prior to installing this patch.

SCADA Expert Vijeo Citect / CitectSCADA customers can download the latest service pack at the following location: http://www.citect.schneider-electric.com/scada/vijeo-citect/downloads-updates/service-packs

3)Will this patch work with any hotfixes installed?

This patch has been created to work for the specific software version & specific service pack. Please check the cumulative hotfix readme for the hotfixes that have been included within this patch. If the hotfixes used on your site match the hotfixes included in this patch then you will need to to uninstall the hotfix prior to applying this patch.

In the event that your site has a different hotfix not included in the patch then please contact support to create a specific hotfix combo to include the hotfixes released in this safety & security patch, for your site.

To check if any hotfix has been installed please go to Control Panel -> Programs -> Programs and Features ->View Installed Updates

4) Which computers should I patch?

Although this vulnerability only affects the server instances, as this patch makes changes in the networking layer we advise that all machines using the product apply the patch. If using the web client the web deployment should be updated with the latest CAB file provided in the patch.

5) 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 subscribe to 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 / Vijeo Historian / CitectHistorian / 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.

©Copyright 2013 Schneider Electric

Schneider Electric shall not be liable for technical or editorial errors or omissions contained herein. The information provided is provided "as is" without warranty of any kind. To the extent permitted by law, neither Schneider Electric or its affiliates, subcontractors or suppliers will be liable for incidental, special or consequential damages including downtime cost; lost profits; damages relating to the procurement of substitute products or services; or damages for loss of data, or software restoration. The information in this document is subject to change without notice. Schneider Electric and the names of the Schneider Electric products referenced herein are trademarks of Schneider Electric in the United States and other countries. Other product and company names mentioned herein may be trademarks of their respective owners