Important security notification – Schneider-Electric Software Update « SESU »

January 11, 2013

Schneider Electric® has become aware of vulnerability on the Schneider-Electric Update Service "SESU".

The vulnerability identified:

The Schneider Electric software suite has a centralized update mechanism for updating Schneider software on a Windows PC. The software on the customer PC uses the update service as the mechanism of communication with the update server in order to receive periodic software updates. This Vulnerability has a non signed communication between the SESU client on the customer PC and the Software Update server. Under certain circumstances and conditions this communication has the potential to execute arbitrary code on a vulnerable system which could result in unexpected consequences. 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 device.

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 to ensure that they can be deployed in a manner that is both safe and secure.

Details on Products Affected

The following products are affected by the use of the SESU mechanism:

Product	Version
IDS 1.0	V1.0
IDS 2.0	V2.
PowerSuite	2.5
Smart Widget Acti 9	V1.0.0.0
Smart Widget H8035	V1.0.0.0
Smart Widget H8036	V1.0.0.0
Smart Widget PM210	V1.0.0.0
Smart Widget PM710	V1.0.0.0
Smart Widget PM750	V1.0.0.0
SoMachine	V1.2.1
Spacial.pro	V 1.0.0.x
SESU	V1.0.x
SESU	V1.1.x

Product	Version
Unity Pro	V7.0 L, M, S, XL
Unity Pro	V6.0 L, M. S, XL
Unity Pro	V6.1 L, M,S, XL
Unity Pro	V5.0 L, M, S, XL
Unity Pro	V4.1 L, M, S, XL, XLS
Vijeo Designer	V6.0.x
Vijeo Designer	V6.1.0.x
Vijeo Designer	V5.0.0.x
Vijeo Designer	V5.1.0.x
Vijeo Designer Opti	V6.0.x
Vijeo Designer Opti	V5.1.0.x
Vijeo Designer Opti	V5.0.0.x
Web Gate Client Files V5.1	V5.1.x

Details on planned fix dates for above described Vulnerability

In order to resolve the Vulnerability with the Software Server, Schneider Electric has taken the following actions:

1. The “SESU server” has been updated to the latest version. Currently both http and https are supported in parallel. Https does ensure signed communication.
2. The new SESU client has been updated as of January 2013 to use https instead of http. The new version of the SESU Client will be made available to customers for distribution via the SESU mechanism in January 2013.
3. Customers can also use an updated software product CD that will contain the updated SESU client, when the CD becomes available. Contact your local support desk for details.
4. While both http and https SESU client functionality is supported currently, several months after starting to update the SESU clients (May 2013) the http port of the SESU server will be disabled. This means that only https will be supported during SESU client updates from that time forward, which mitigates this current vulnerability.

General Recommendations

Schneider Electric has been designing industrial automation products for many years; Schneider Electric follows, and recommends to its customers, industry best practices in the development and implementation of control systems. This recommendation includes a Defense in Depth approach to secure an Industrial Control System. This approach places the PLCs behind one or more firewalls to restrict access to authorized personnel and protocols only. The location of the firewalls is decided based on how large the trusted zone is required to be. Please read the following document for more detailed information:

http://download.schneider-electric.com/files?p_File_Id=25779912&p_File_Name=Cyber-Security-STN-v2-Aug-2012.pdf

Acknowledgments

Schneider Electric wishes to thank researcher Arthur Gervais for reporting of the vulnerabilities and working with Schneider during the disclosure process

Support CVSS Scoring

CVSS scores are a standard way of ranking vulnerabilities and are provided for reference based on a typical control system they should be adapted by individual users as required.

CVSS Base Score:9.3 AV:N/AC:M/Au:N/C:C/I:C/A:C