Improper Access Control Vulnerability in MicroSCADA Pro SYS600 9.x

ABBVU-PGGA-33888

Update Date:
3.2.2018 Original document
16.3.2018 Fix for SYS600 9.3 systems is available. Clarified file system permissions for created Windows groups, see FAQ.

Notice

The information in this document is subject to change without notice, and should not be construed as a commitment by ABB.

ABB provides no warranty, express or implied, including warranties of merchantability and fitness for a particular purpose, for the information contained in this document, and assumes no responsibility for any errors that may appear in this document. In no event shall ABB or any of its suppliers be liable for direct, indirect, special, incidental or consequential damages of any nature or kind arising from the use of this document, or from the use of any hardware or software described in this document, even if ABB or its suppliers have been advised of the possibility of such damages.

This document and parts hereof must not be reproduced or copied without written permission from ABB, and the contents hereof must not be imparted to a third party nor used for any unauthorized purpose.

All rights to registrations and trademarks reside with their respective owners.

Affected Products

All MicroSCADA Pro SYS600 9.x versions.

Vulnerability ID

ABB ID: ABBVU-PGGA-33888

CVE ID: CVE-2018-1168

Summary

ABB is aware of private reports of a vulnerability. An update is available that resolves a privately reported vulnerability.

The vulnerability is in Windows file system permissions (ACL, access control lists). The fix is to change the file system permissions of SYS600 installation directory.

To exploit this vulnerability and to install a malicious file in the server, the attacker must first gain access to the file system via physical access or authenticate to local account.

Vulnerability Severity

The severity assessment has been performed by using the FIRST Common Vulnerability Scoring System (CVSS) for both CVSS v2 and v3. The CVSS Environmental Score, which can affect the vulnerability severity, is not provided in this advisory since it reflects the potential impact of a vulnerability within the end-user organizations' computing environment; end-user organizations are therefore recommended to analyze their situation and specify the Environmental Score.

CVSS v2 Base Score: 6.0
CVSS v2 Temporal Score: 4.4
CVSS v2 Vector: AV:L/AC:H/Au:S/C:C/I:C/A:C/E:U/RL:OF/RC:C)
CVSS v2 Link: https://nvd.nist.gov/vuln-metrics/cvss/v2-calculator?version=2&vector=(AV:L/AC:H/Au:S/C:C/I:C/A:C/E:U/RL:OF/RC:C)

CVSS v3 Base Score: 6.4 (Medium)
CVSS v3 Temporal Score: 5.6 (Medium)
CVSS v3 Vector: AV:L/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C
CVSS v3 Link: https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C

Corrective Action or Resolution

To resolve this vulnerability, file system permissions needs to be changed in SYS600 installation directory.

SYS600 9.3 **SYS600 9.3 FP3** **SYS600 9.4** **SYS600 9.4 FP1** **SYS600 9.4 FP2**	Fix is available. Instructions in the technical document, see link below.
SYS600 9.2 **SYS600 9.1** **SYS600 9.0**	No fix available. Customers are recommended to upgrade to the latest SYS600 version.

Technical document: See link.

ABB recommends that customers apply above procedures at the earliest convenience.

Vulnerability Details

The vulnerability is in Windows file system permissions (ACL, access control lists). The fix is to change the file system permissions of SYS600 installation directory. Access control enforces policy such that users cannot act outside of their intended permissions. For example, in Windows operating systems non-admin users should not have possibility to add files to the product installation directory containing executables/binaries.

SYS600 installation directory have improper access control, which makes possible for all authenticated non-admin Windows users in the server to add files and run arbitrary code and possibly escalate privileges. An attacker who successfully exploited this vulnerability could run arbitrary code in the server and get full privileges.

To install a malicious file, the attacker must first gain access to the file system of the server via physical access or successfully authenticating to Windows operating systems.

Mitigating Factors

Recommended security practices and firewall configurations can help protect a process control network from attacks that originate from outside the network. Such practices include that process control systems are physically protected from direct access by unauthorized personnel, have no direct connections to the Internet, and are separated from other networks by means of a firewall system that has a minimal number of ports exposed, and others that have to be evaluated case by case. Process control systems should not be used for Internet surfing, instant messaging, or receiving e-mails. Portable computers and removable storage media should be carefully scanned for viruses before they are connected to a control system.

More information on recommended practices can be found in the ICS-CERT documents.

Frequently asked questions

What is the scope of the vulnerability?
An attacker who successfully exploited this vulnerability could insert and run arbitrary code in an affected system node.

What causes the vulnerability?
The vulnerability is caused by improper file system permissions in product installation directory in Windows operating system.

What might an attacker use the vulnerability to do?
An attacker who successfully exploited this vulnerability could elevate privileges of non-admin user and take control of the affected system node.

How could an attacker exploit the vulnerability?
An attacker could try to exploit the vulnerability by creating a specially crafted file and copy the file to an affected system node. This would require that the attacker has physical access to the affected system node or to Windows user account in that node. Recommended practices help mitigate such attacks, see section Mitigating Factors above.

Could the vulnerability be exploited remotely?
No, to exploit this vulnerability an attacker would need to have physical access or Windows user account to an affected system node.

What does the fix do?
The fix configures stricter file system permissions so that not all non-admin users (Users, Authenticated Users) are getting by default ability to add files to the directories containing executable files. Instead, more permissions are given to specific Windows groups e.g. ScEngineers. This gives full access rights to specific product directories for a non-admin user being a member of this group but still gives better protection when an engineer can use the product with less privileges and membership of Administrators group is not required that would give full control to the system node.

When this security advisory was issued, had this vulnerability been publicly disclosed?
No, ABB received information about this vulnerability through responsible disclosure.

When this security advisory was issued, had ABB received any reports that this vulnerability was being exploited?
No, ABB had not received any information indicating that this vulnerability had been exploited when this security advisory was originally issued.

Acknowledgements

ABB thanks the following for working with us to help protect customers:

- Fritz Sands of Trend Micro Zero Day Initiative (ZDI) for reporting this vulnerability

Support

For additional information and support please contact your local ABB service organization. For contact information, see www.abb.com.

Information about ABB's cyber security program and capabilities can be found at www.abb.com/cybersecurity.