Pro-face by Schneider Electric

Security Notification – GP-Pro EX – Updated on 1-Apr-2016

3/14/2016

Overview

Digital Electronics/Pro-face has become aware of multiple vulnerabilities in GP-Pro EX.

The vulnerabilities identified include:

	Contents	CVSS v3 Score	CVE ID
1	Stack Buffer Overflow Remote Code – Execution	7.3, (AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L)	CVE-2016-2292
2	Out-Of-Bounds Read Information Disclosure	5.3, (AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N)	CVE-2015-2291
3	In the D-Script function, Heap Buffer Overflow Remote Code Execution	6.3, (AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L)	CVE-2015-2290
4	In the “Transfer Tool”, Hardcoded credentials on the FTP server that enable access to the project data information.	9.1, (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N)	CVE-2015-7921
5	In the “Transfer Tool”, Possible Secondary Authentication Bypass that enable access to the project data information	9.1, (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N)	CVE-2015-7921

Vulnerabilities Overview

Pro-face would like to thank Steven Seeley of Source Incite, working with HP's Zero Day Initiative (ZDI) for items 1-3, and independent researcher Jeremy Brown for items 4-5.

Pro-face is not aware of any of these vulnerabilities having been exploited.

ZDI published advisories CVE-2016-2292, CVE-2015-2291, and CVE-2015-2290 regarding 3 vulnerabilities that may allow remote attackers to disclose information on vulnerable installations of GP-Pro EX. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file.

In addition, the 2 vulnerabilities related to “Transfer Tool” may allow remote attackers access to project data information, however, write access to the HMI is not available, and the PRX project files are encrypted, making them difficult to modify or create.

Product(s) Affected

HMI Screen Editor & Logic Programing Software “GP-Pro EX ":

Product model:	EX-ED*,PFXEXEDV*,PFXEXEDLS*,PFXEXGRPLS*
Applicable version:	GP Pro EX Ver. 1.00 to Ver. 4.0.4
How to check the version:	[Help (H)] → [About this program (A)]

Workaround and Solution

The following modules are released.

-> GP-Pro EX (Ver. 4.05.000 or later) Update Module including

Editor: Ver.4.05.000

Transfer Tool: Ver.4.05.000

System/Runtime: Ver.4.5.0

* To download the module, free member registration for “Otasuke Pro!” is required.

Mitigation

Customers are also advised to take the following measures to help minimize exploitation risk:

- Review all network configurations for control system devices
  - Remove unnecessary PC(s) from control system networks
  - Remove unnecessary applications from control system networks
- Minimize network exposure for all control system devices. Control system devices should not have a direct connection to the Internet.
- Configure control system networks and devices behind firewalls. Isolate the control systems from business networks.
- When remote access to a control system is required, employ secure methods, such as Virtual Private Networks (VPNs), while keeping in mind that a VPN is only as secure as the connected devices.

For More Information

This document is intended to help provide an overview of the identified vulnerability and actions to mitigate it. To obtain full details on the issues, and assistance on how to protect your installation, please contact your local Digital Electronics/Pro-face representative. These organizations will be fully aware of the situation and can support you through the process.

Product Security Office

Digitally signed by Product Security Office
DN: cn=Product Security Office, o=Schneider Electric, ou=Global Technology, email=cybersecurity@schneider-electric.com, c=US
Date: 2016.04.01 15:44:11 -04'00'