# Web Studio Security Bulletin

## Remote Code Execution and Remote Arbitrary Command Execution Vulnerabilities

**Rating** - Critical

**Overview**

A security update has been issued to address vulnerabilities in Web Studio v8.0 SP2 Patch 1 and prior versions. The vulnerabilities, if exploited, could allow an un-authenticated malicious entity to remotely execute code and/or arbitrary commands with high privileges. It is recommended that organizations evaluate the impact of these vulnerabilities based on their operational environment, architecture, and product implementation.

**Recommendations**

Customers using Web Studio v8.0 SP2 Patch 1 or prior versions are affected and should upgrade and apply Web Studio v8.1 as soon as possible.

**Background**

Web Studio is a powerful collection of tools that provide all the automation building blocks to develop HMIs, SCADA systems and embedded instrumentation solutions.

To identify which version of Web Studio you have installed:

- On a Windows Desktop or Server operating system, navigate to Windows Programs and Features, locate the “SoftPLC Web Studio” entries and observe the displayed installed version.
- On a Windows Embedded/CE operating system, navigate to the Bin folder in the installation location of Web Studio and open the file “CEView.ini”. The installed version can be observed from the “version=*.*.*” attribute within the file.

**Vulnerability Details**

1) Web Studio provides the capability for an HMI client to subscribe to tags and monitor their values. A remote malicious entity could send a carefully crafted packet to exploit a stack-based buffer overflow vulnerability during tag subscription, with potential for code to be executed. The code would be executed under high privileges and could lead to a complete compromise of the Web Studio server machine.

2) Web Studio provides the capability for an HMI client to trigger script execution on the server for the purposes of performing customized calculations or actions. A remote malicious entity could bypass the server authentication and trigger an arbitrary command to be executed. The command is executed under high privileges and could lead to a complete compromise of the server machine.

**Security Update**
Web Studio v8.1 Security Update addresses the vulnerabilities outlined in this Security Bulletin.

**Vulnerability Characterization and CVSSv3 Rating**
CWE-121: Stack-based Buffer Overflow
9.8 | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CWE-306: Missing Authentication for Critical Function
9.8 | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

**Cyber Security Standards and Best Practices**
For information regarding how to secure Industrial Control Systems please reference NIST SP800-82r2.

NVD Common Vulnerability Scoring System (CVSS v3)
The U.S. Department of Homeland Security has adopted the common Vulnerability Scoring System (CVSS v3) that provides an open framework for communicating the characteristics and impacts of IT vulnerabilities. CVSS v3 produces a numerical score as well as a textual representation of that score reflecting the severity of a vulnerability. Scores range from 0.0 (no impact) to a maximum of 10.0 (critical impact with minimal effort to exploit). For additional information please refer to the CVSSv3 specifications.

Disclaimer
THE INFORMATION PROVIDED HEREIN IS PROVIDED “AS-IS” AND WITHOUT WARRANTY OF ANY KIND. SOFTPLC CORPORATION DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. NO ORAL OR WRITTEN INFORMATION OR ADVICE GIVEN BY SOFTPLC CORPORATION, ITS DEALERS, DISTRIBUTORS, AGENTS OR EMPLOYEES WILL CREATE A WARRANTY AND CUSTOMER MAY NOT RELY ON ANY SUCH INFORMATION OR ADVICE.

SOFTPLC CORPORATION DOES NOT WARRANT THAT THE SOFTWARE WILL MEET CUSTOMER’S REQUIREMENTS, THAT THE SOFTWARE WILL OPERATE IN COMBINATIONS OTHER THAN AS SPECIFIED IN SOFTPLC'S DOCUMENTATION OR THAT THE OPERATION OF THE SOFTWARE WILL BE UNINTERRUPTED OR ERROR-FREE.

IN NO EVENT WILL SOFTPLC CORPORATION OR ITS SUPPLIERS, DEALERS, DISTRIBUTORS, AGENTS OR EMPLOYEES BE LIABLE FOR ANY INDIRECT, INCIDENTAL, SPECIAL, PUNITIVE OR CONSEQUENTIAL DAMAGES, OR DAMAGES FOR LOSS OF PROFITS, REVENUE, DATA OR USE, INCURRED BY CUSTOMER OR ANY THIRD PARTY, WHETHER IN AN ACTION IN CONTRACT OR TORT, EVEN IF SOFTPLC CORPORATION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SOFTPLC CORPORATION’S LIABILITY FOR DAMAGES AND EXPENSES HEREUNDER OR RELATING HERETO (WHETHER IN AN ACTION IN CONTRACT, TORT OR OTHERWISE) WILL IN NO EVENT EXCEED THE AMOUNT OF ONE HUNDRED DOLLARS ($100 USD).