## SSA-451236: Vulnerability in SIMATIC ProSave, SIMATIC CFC, SIMATIC STEP 7, SIMOTION Scout, and STARTER

| | |
|---|---|
| Publication Date | 2015-03-05 |
| Last Update | 2015-04-22 |
| Current Version | V1.1 |
| CVSS Overall Score | 5.4 |

Summary:

The latest updates for the affected products fix a vulnerability that could allow attackers with local access to the system to execute arbitrary code under certain conditions.

## AFFECTED PRODUCTS

- SIMATIC ProSave: All versions < V13 SP1
- SIMOTION Scout: All versions < V4.4
- STARTER: All versions < V4.4 HF3
- SIMATIC CFC
  - All versions prior to V8.0 SP4
  - CFC V8.0 SP4: All versions < V8.0 SP4 Upd 9
  - CFC V8.1: All versions < V8.1 Upd1
- SIMATIC STEP 7 V5.5
  - All versions prior to V5.5 SP1
  - STEP 7 V5.5 SP1: All versions < V5.5 SP1 HF2
  - STEP 7 V5.5 SP2: All versions < V5.5 SP2 HF7
  - STEP 7 V5.5 SP3: All versions < V5.5 SP3 HF10
  - STEP 7 V5.5 SP4: All versions < V5.5 SP4 HF4
- SIMATIC PCS 7 (as STEP 7 and CFC are incorporated)
  - All versions prior to V8.0 SP2
  - PCS 7 V8.0 SP2: All versions < V8.0 SP2 with STEP 7 V5.5 SP3 HF10 and CFC V8.0 SP4 Upd9
  - PCS 7 V8.1: All versions < V8.1 with STEP 7 V5.5 SP4 HF4 and CFC V8.1 Upd1

## DESCRIPTION

SIMATIC ProSave is used for backup restore and firmware update for SIMATIC HMI panels.

SIMOTION SCOUT is the framework for all motion control engineering system tools.

STARTER is the drive engineering tool for parameterizing and commissioning.

SIMATIC CFC (Continuous Function Chart) is a graphic editor which is a core component of PCS 7 engineering systems and optionally available for STEP 7.

STEP 7 is Siemens' classic engineering software for PLC and hardware configuration.

SIMATIC PCS 7 is a distributed control system (DCS) integrating SIMATIC STEP 7 and SIMATIC CFC.

Detailed information about the vulnerability is provided below.

## VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSSv2 scoring system (http://www.first.org/cvss/). The CVSS environmental score is specific to the customer's environment and will impact the overall CVSS score. The environmental score should therefore be individually defined by the customer to accomplish final scoring.

### Vulnerability Description (CVE-2015-1594)

Insufficiently qualified paths could allow attackers to execute arbitrary code from files located on the local file system or connected network shares with the privileges of the user running the affected products. For successful exploitation an unsuspecting user must be tricked into opening a manipulated application file.

| | |
|---|---|
| CVSS Base Score | 6.9 |
| CVSS Temporal Score | 5.4 |
| CVSS Overall Score | 5.4 (AV:L/AC:M/Au:N/C:C/I:C/A:C/E:POC/RL:OF/RC:C) |

### Mitigating factors

For successful exploitation of the vulnerability an attacker must:

- have write access to the local file system or connected network shares, and
- be able to trick a legitimate user to open a malicious application file (e.g. by social engineering)

## SOLUTION

Siemens provides updates for the following products and recommends customers to update to the new fixed versions:

- SIMATIC ProSave: Update to version V13 SP1 [1]
- SIMOTION Scout: Update to version 4.4 [2]
- STARTER: Update to version 4.4 HF3 [3]
- SIMATIC CFC:
  - CFC V8.0 SP4: Update to V8.0 SP4 Upd9 [4]
  - CFC V8.1: Update to V8.1 Upd1 [4]
- SIMATIC STEP 7 V5.5:
  - STEP 7 V5.5 SP1: Update to V5.5 SP1 HF2 [4]
  - STEP 7 V5.5 SP2: Update to V5.5 SP2 HF7 [4]
  - STEP 7 V5.5 SP3: Update to V5.5 SP3 HF10 [4]
  - STEP 7 V5.5 SP4: Update to V5.5 SP4 HF4 [4]
- SIMATIC PCS 7 V8.0 SP2:
  - CFC V8.0 SP4: Update to V8.0 SP4 Upd9 [4]
  - STEP 7 V5.5 SP3: Update to V5.5 SP3 HF10 [4]
- SIMATIC PCS 7 V8.1:
  - CFC V8.1: Update to V8.1 Upd1 [4]
  - STEP 7 V5.5 SP4: Update to V5.5 SP4 HF4 [4]

For versions of SIMATIC CFC prior to V8.0 and SIMATIC PCS 7 prior to V8.0 Siemens recommends upgrading to the most recent software versions.

Until customers can apply the updates, Siemens recommends customers to mitigate the risk of their products by implementing the following steps:

- Do not load or use files from untrusted parties
- Ensure that only trustworthy persons have access to the system
- Apply whitelisting solutions to the system according to the operational guidelines [5]

As a general security measure Siemens strongly recommends to protect network access with appropriate mechanisms. It is advised to configure the environment according to our operational guidelines [5] in order to run the devices in a protected IT environment.

## ACKNOWLEDGEMENT

Siemens thanks Ivan Sanchez from WiseSecurity Team for coordinated disclosure of the vulnerability.

## ADDITIONAL RESOURCES

[1] The update for SIMATIC ProSave can be obtained here: https://support.industry.siemens.com/cs/de/en/view/10347815

[2] The update for SIMOTION Scout can be obtained here: https://support.industry.siemens.com/cs/de/en/view/107586911

[3] The update for STARTER can be obtained here: https://support.industry.siemens.com/cs/ww/en/view/26233208

[4] Updates for SIMATIC STEP 7 and SIMATIC CFC can obtained via customer support: http://www.siemens.com/automation/support-request

[5] An overview of the operational guidelines for Industrial Security (with the cell protection concept): https://www.siemens.com/cert/operational-guidelines-industrial-security

[6] Information about Industrial Security by Siemens: http://www.siemens.com/industrialsecurity

[7] For further inquiries on vulnerabilities in Siemens products and solutions, please contact the Siemens ProductCERT: http://www.siemens.com/cert/advisories

## HISTORY DATA

| | |
|---|---|
| V1.0 (2015-03-05): | Publication Date |
| V1.1 (2015-04-22): | Added fix for STEP 7 V5.5 SP3 and PCS 7 V8.0 SP2 |

## DISCLAIMER

See: http://www.siemens.com/terms_of_use