SSA-523365: Vulnerability in SIMATIC PCS 7

Publication Date: 2017-10-18
Last Update: 2018-06-12
Current Version: V1.1
CVSS v3.0 Base Score: 4.9

SUMMARY
The latest software update for SIMATIC PCS 7 fixes a vulnerability, which could allow an attacker to cause a Denial-of-Service (DoS) condition under certain circumstances.

AFFECTED PRODUCTS AND SOLUTION

<table>
<thead>
<tr>
<th>Affected Product and Versions</th>
<th>Remediation</th>
</tr>
</thead>
<tbody>
<tr>
<td>All versions &lt; V8.1 SP1 with WinCC V7.3 Upd 13</td>
<td></td>
</tr>
<tr>
<td>SIMATIC PCS 7 V8.2:</td>
<td>Update to V8.2 SP1</td>
</tr>
<tr>
<td>All versions &lt; V8.2 SP1</td>
<td>To obtain SIMATIC PCS 7 V8.2 SP1 contact your local support.</td>
</tr>
</tbody>
</table>

WORKAROUNDS AND MITIGATIONS
Siemens has identified the following specific workarounds and mitigations that customers can apply to reduce the risk:

- Apply cell protection concept
- Use VPN for protecting network communication between cells
- Apply Defense-in-Depth

GENERAL SECURITY RECOMMENDATIONS
As a general security measure, Siemens strongly recommends to protect network access to devices with appropriate mechanisms. In order to operate the devices in a protected IT environment, Siemens recommends to configure the environment according to Siemens’ operational guidelines for Industrial Security (Download: [https://www.siemens.com/cert/operational-guidelines-industrial-security](https://www.siemens.com/cert/operational-guidelines-industrial-security)), and to follow the recommendations in the product manuals.

Additional information on Industrial Security by Siemens can be found at: [https://www.siemens.com/industrialsecurity](https://www.siemens.com/industrialsecurity)

PRODUCT DESCRIPTION
SIMATIC WinCC is a supervisory control and data acquisition (SCADA) system.
SIMATIC PCS 7 is a distributed control system (DCS) integrating SIMATIC WinCC, SIMATIC Batch, SIMATIC Route Control, OpenPCS7 and other components.
VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.0 (CVSS v3.0) (https://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 CVE-2017-6867

An authenticated, remote attacker who is member of the “administrators” group could crash services by sending specially crafted messages to the DCOM interface.

<table>
<thead>
<tr>
<th>CVSS v3.0 Base Score</th>
<th>4.9</th>
</tr>
</thead>
</table>

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Sergey Temnikov and Vladimir Dashchenko from Critical Infrastructure Defense Team, Kasperky Lab for coordinated disclosure of the vulnerability

ADDITIONAL INFORMATION

For further inquiries on security vulnerabilities in Siemens products and solutions, please contact the Siemens ProductCERT:

https://www.siemens.com/cert/advisories

HISTORY DATA

V1.0 (2017-10-18): Publication Date
V1.1 (2018-06-12): Update of PCS 7 V8.2

TERMS OF USE

Siemens Security Advisories are subject to the terms and conditions contained in Siemens’ underlying license terms or other applicable agreements previously agreed to with Siemens (hereinafter “License Terms”). To the extent applicable to information, software or documentation made available in or through a Siemens Security Advisory, the Terms of Use of Siemens’ Global Website (https://www.siemens.com/terms_of_use, hereinafter "Terms of Use"), in particular Sections 8-10 of the Terms of Use, shall apply additionally. In case of conflicts, the License Terms shall prevail over the Terms of Use.