SSA-804859: Denial of Service Vulnerability in SIMATIC Logon

Publication Date 2017-07-06
Last Update 2017-07-06
Current Version V1.0
CVSS v3.0 Base Score 5.3

SUMMARY

The latest version of SIMATIC Logon fixes a security vulnerability that could allow attackers to cause a denial of service of the SIMATIC Logon Remote Access service under certain conditions.

AFFECTED PRODUCTS

- SIMATIC Logon: All versions < V1.6

DESCRIPTION

The SIMATIC Logon Remote Access service provides authentication for access control on SIMATIC HMI panels. The Remote Access service is an optional component of SIMATIC Logon (SL) that is used for central user administration and access control in other SIMATIC applications.

Detailed information about the vulnerability is provided below.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.0 (CVSS v3.0) (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 assessed by the customer to accomplish final scoring.

Vulnerability (CVE-2017-9938)

Specially crafted packets sent to the SIMATIC Logon Remote Access service on port 16389/tcp could cause a Denial-of-Service condition. The service restarts automatically.

CVSS Base Score 5.3
CVSS Vector CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RL:O/RC:C

Mitigating Factors

The SIMATIC Logon Remote Access is only used in conjunction with SIMATIC HMI panels.

The attacker must have network access to the affected service. Siemens recommends operating the service only within trusted networks [2].

SOLUTION

Siemens provides software upgrade V1.6 [1] for SIMATIC Logon which fixes the vulnerability and recommends customers upgrade to the newest version.

As a general security measure Siemens strongly recommends protecting network access to the port 16389/tcp of the SIMATIC Logon Remote Access service with appropriate mechanisms. It is advised to configure the environment according to our operational guidelines [3] in order to run the devices in a protected IT environment.

ACKNOWLEDGEMENTS

Siemens thanks Tenable Network Security for coordinated disclosure of the vulnerability.

ADDITIONAL RESOURCES

[1] SIMATIC Logon V1.6 can be obtained via your local Siemens representative or customer support:
https://www.siemens.de/automation/partner

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

[3] Information about Industrial Security by Siemens:
https://www.siemens.com/industrialsecurity

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

HISTORY DATA

V1.0 (2017-07-06): Publication Date

DISCLAIMER