OpenSource Security Ralf Spenneberg

Am Bahnhof 3-5

48565 Steinfurt

info@os-s.net

OS-S Security Advisory 2016-20

Date: March 14th, 2016

Last Updated: March 14th, 2016

Authors: Maik Brüggemann, Hendrik Schwartke, Ralf Spenneberg

CVE: CVE-2016-2846

CVSS: 6.5 (AV:N/AC:L/Au:N/C:P/I:P/A:N)

Title: Know-How and Copy Protection may be circumvented on S7-1200 version 1 through 3.

Severity: Critical.

Vendor contacted: October 9th 2015

Ease of Exploitation: Knowledge of the protocol required

Vulnerability type: Wrong usage of password mechanism

Products: S7 1200 versions 1 through 3. Version 4 is not affected.

Abstract

The S7 1200 offers three different protection modes. Both the know-how protection and the copy protection use a password to protect the stored user program. Both mechanisms may be circumvented by an attacker.

Solution:

Upgrade to Version 4.

References:

http://www.siemens.com/cert/pool/cert/siemens_security_advisory_ssa-833048.pdf