SSL 3.0 Protocol Vulnerability and POODLE Attack in Protection and Control IED Manager PCM600

ABB-VU-PPMV-1MRS758303

Notice

The information in this document is subject to change without notice, and should not be construed as a commitment by ABB.

ABB provides no warranty, express or implied, including warranties of merchantability and fitness for a particular purpose, for the information contained in this document, and assumes no responsibility for any errors that may appear in this document. In no event shall ABB or any of its suppliers be liable for direct, indirect, special, incidental or consequential damages of any nature or kind arising from the use of this document, or from the use of any hardware or software described in this document, even if ABB or its suppliers have been advised of the possibility of such damages.

This document and parts hereof must not be reproduced or copied without written permission from ABB, and the contents hereof must not be imparted to a third party nor used for any unauthorized purpose.

All rights to registrations and trademarks reside with their respective owners.

Affected Products

PCM600 Ver. 2.5 and Ver. 2.6 are affected.

Summary

A vulnerability has recently been published that affects the SSL protocol 3.0 and is commonly referred to as “POODLE”. The vulnerability affects the product versions listed above.

Additional Information can be found here:

- http://www.kb.cert.org/vuls/id/577193

A published vulnerability CVE-2014-8730 referring to "POODLE" that concerns also the TLS protocol does not affect PCM600 versions.

Severity rating

The severity rating for this vulnerability is important, with the overall CVSS score 4.3. This assessment is based on the types of systems that are affected by the vulnerability, how difficult it is to exploit, and the effect that a successful attack exploiting the vulnerability could have.

CVSS Overall Score: 4.3

CVSS Vector: *(AV:N/AC:M/Au:N/C:P/I:N/A:N)*

CVSS Link: https://nvd.nist.gov/cvss.cfm?version=2&name=CVE-2014-3566&vector=(AV:N/AC:M/Au:N/C:P/I:N/A:N)

Corrective Action or Resolution

ABB has investigated this vulnerability and is working towards several corrective packages to provide adequate protection to customers.
There are following corrective packages available:

- PCM600 2.6 Hotfix Rollup 20150511 to update the latest PCM600 Ver. 2.6 (SSL 3.0 will get disabled in the FTPS communication with mentioned IEDs)
- IED maintenance releases for 650 Ver. 1.3.0 / 1.3.0.1 and for 615 Ver. 5.0.0 – 5.0.4 (see related separate advisories for the affected Relion series IEDs)

Based on the customers risk assessment and exposure of the system, the available IED maintenance releases and the upcoming PCM600 hotfix package for Ver. 2.6, expected by Q1/Q2 2015, should be applied.

ABB recommends that customers also follow the steps outline in the section “Mitigating Factors”.

Customers shall contact their local ABB contacts to obtain the maintenance release. For updating the PCM600 software, the PCM600 Update Manager shall be used to download and install the recommended PCM600 2.6 Rollup 20150511.

Vulnerability Details

A new vulnerability has been discovered in the SSL protocol 3.0. To work with legacy servers, many TLS clients implement a downgrade operation: In a first handshake attempt, TLS clients offer the highest protocol version supported by them; if this handshake fails, retry (possibly repeatedly) with earlier protocol versions. This downgrade can also be triggered by network glitches, and by active attackers. If an attacker that controls the network between the client and the server interferes with any attempted handshake offering TLS 1.0 or later, such clients/servers will readily confine themselves to SSL 3.0.

The SSL protocol 3.0, as used in the openSSL cryptographic software library uses nondeterministic CBC padding, which make it easier for man-in-the-middle attackers to obtain clear text data via padding-oracle attack aka, POODLE attack (Padding Oracle On Downgraded Legacy Encryption).

CVE-2014-3566 is the official reference to this bug. CVE (Common Vulnerabilities and Exposures) is the Standard for Information Security Vulnerability Names maintained by MITRE.

Mitigating Factors

Recommended security practices and firewall configurations can help protect an industrial control network from attacks that originate from outside the network. Such practices include that industrial control systems are physically protected from direct access by unauthorized personnel, have no direct connections to the Internet, and are separated from other networks by means of a firewall system that has a minimal number of ports exposed, and others that have to be evaluated case by case. Industrial control systems should not be used for Internet surfing, instant messaging, or receiving e-mails. Portable computers and removable storage media should be carefully scanned for viruses before they are connected to a control system.

Workarounds

Workarounds are described in the *Corrective Action or Resolution* chapter above.

Frequently asked questions

What is the scope of the vulnerability?
An attacker who successfully exploits this vulnerability could get hold of the user credentials and cryptographic keys used to login to the device.

What causes the vulnerability?
A bug in the protocol SSL 3.0 causes the vulnerability.

What is the affected product or component?
FTPS in PCM600 Ver. 2.5 and Ver. 2.6 uses SSL 3.0 for the secure communication with the following IED series:

- Relion 650 series Ver. 1.3.0 and Ver. 1.3.0.1
- Relion 615 series Ver. 5.0.0 – 5.0.4

What might an attacker use the vulnerability to do?
An attacker who successfully exploits this vulnerability could get hold of the user credentials and cryptographic keys used to access the device.

How could an attacker exploit the vulnerability?

An attacker could try to exploit the vulnerability by creating a specially crafted message and sending the message to an affected system node. This would require that the attacker has access to the system network, by connecting to the network either directly or through a wrongly configured or penetrated firewall, or that he installs malicious software on a system node or otherwise infects the network with malicious software. Recommended practices help mitigate such attacks, see section Mitigating Factors above.

Could the vulnerability be exploited remotely?
Yes, an attacker who has network access to an affected system node or has the possibility to be the man-in-the-middle could exploit this vulnerability. Recommended practices include that industrial control systems are physically protected, have no direct connections to the Internet, and are separated from other networks by means of a firewall system that has a minimal number of ports exposed.

When this security advisory was issued, had this vulnerability been publicly disclosed?
Yes, this vulnerability has been publicly disclosed.

When this security advisory was issued, had ABB received any reports that this vulnerability was being exploited?
No, ABB had not received any information indicating that this vulnerability had been exploited in PCM600 when this security advisory was originally issued.

Support

For additional information and support please contact your local ABB service organization. For contact information, see www.abb.com/substationautomation.

Information about ABB’s cyber security program and capabilities can be found at www.abb.com/cybersecurity.