SSL 3.0 Protocol Vulnerability and POODLE Attack in COM600

ABB-VU-PPMV-1MRS758302

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.

Affected Products

COM600 versions 3.0, 3.1, 3.2, 3.3, 3.4, 3.5 and 4.0

Summary

Vulnerability has recently been published that affects the SSL protocol 3.0 and is commonly referred to as “POODLE”. The vulnerability affects the above mentioned product versions encrypted HTTPS communication for WebHMI service.

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 COM600 versions.

Severity rating

The severity rating for this vulnerability is Medium, 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 (Medium)

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 have now published instructions how to disable SSL 3.0 in affected COM600 versions which fixes the reported issue.

Fix can be applied for COM600 Operating System according following Microsoft KB article for this subject: http://support.microsoft.com/KB/187498

Or with following procedure:

- Create new file in COM600 file system named as disable_ssl3.reg and copy next lines to it.

```
Windows Registry Editor Version 5.00


[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\
PCT 1.0]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\
PCT 1.0\Server]

"Enabled"=dword:00000000

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\
SSL 2.0]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\
SSL 2.0\Client]

"DisabledByDefault"=dword:00000001

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\
SSL 2.0\Server]

"Enabled"=dword:00000000

"DisabledByDefault"=dword:00000001

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\
SSL 3.0]
```

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\Client]

"DisabledByDefault"=dword:00000001

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\Server]

"Enabled"=dword:00000000

- Save the file to COM600 file system and run it

Based on the customers risk assessment and exposure of the system, the corrective action should be applied.

ABB recommends that customers also follow the steps outline in the sections “Mitigating Factors” and “Workarounds”.

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 either upgrading protection relay firmware or using HTTPS clients with TLS option only.

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. This requires attacker to get access to communication node or communication channel between client and server and analyze the SSL 3.0 traffic.

What causes the vulnerability?
The vulnerability is caused by a bug in the protocol SSL 3.0 that is used in the COM600.

What is the affected product or component?
In the COM600 affected product versions, the affected component is WebHMI service which can use the SSL 3.0 protocol in HTTPS.

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 the COM600 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/medium-voltage.

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