# Yokogawa Security Advisory Report

YSAR-14-0005E
Published on December, 5, 2014
Last updated on December 22, 2017

## YSAR-14-0005E: SSLv3 protocol vulnerability of decrypting the encrypted data in YOKOGAWA products

### Overview:

A vulnerability has been found with YOKOGAWA products of supporting SSLv3 protocol. The vulnerability allows decrypting a part of the communication data encrypted by SSLv3. Yokogawa identified the range of products that could be influenced by the vulnerability in this document.

Go over the report and confirm which products are affected in order to consider security measures for the overall systems. Also please consider applying the countermeasures as needed.

### Affected Products:

Following are the products that would be affected by the vulnerability reported in this document.

- Exaquantum (R2.80 and R2.85)
- Exaquantum/Batch (R2.50.30 and 2.50.40)
- Exasmoc, Exarqe (from R4.01.00 to R4.03.20) (*1)
- FAST/TOOLS (from 9.01 to 10.01SP2）
- GX10/GX20, GP10/GP20 (from R2.01.01 to R2.02.01) (*2)
- GM10 (R2.02.01) (*2)
- DTSX200 (KernelBuildNo R1.06.01 or earlier）
- DTSX3000 (KernelBuildNo R1.07.01)
- e-fabDoctor Passport （R4.1 or earlier）

(*1) This product is affected by this vulnerability if SSL enabled on the Web function.
(*2) These products are affected by this vulnerability if SSL enabled on the server function(FTP, WEB) or the client function(FTP, SMTP).

### Vulnerability - SSLv3 protocol vulnerability:

For a communication encrypted by SSLv3 CBC mode between an affected product and another computer, a part of the communication data allows to be decrypted by cut in on between the two communicating entities.
As a result, there is a possibility of information disclosure.

When the system-wide network is properly managed (i.e., when the affected product(s) is/are on an isolated network), the risk of exploiting this vulnerability could be low because it is difficult to cut in on between the two communicating entities by attackers.

CVSS Base Score: 4.3, Temporal Score: 3.7

| | |
|---|---|
| Access Vector: | Network |
| Access Complexity: | Medium |
| Authentication: | None |
| Confidentiality Impact (C): | Partial |
| Integrity Impact (I): | None |

| | |
|---|---|
| Availability Impact (A): | None |
| Exploitability: | Functional |
| Remediation Level: | Temporary Fix |
| Report Confidence: | Confirmed |

## Countermeasures:

Please contact the supports in the following section for the countermeasures regarding the affected products.

Yokogawa strongly suggests all customers to introduce appropriate security measures not only for the vulnerabilities identified but also to the overall systems.

## Supports:

For questions related to this document, please contact the below.

- Exaquantum, Exaquantum/Batch, Exasmoc, Exarqe
  https://contact.yokogawa.com/cs/gw?c-id=000007
- FAST/TOOLS
  https://contact.yokogawa.com/cs/gw?c-id=000037
- GX10/GX20, GP10/GP20, GM10
  https://y-link.yokogawa.com/YL006/index3
- DTSX200, DTSX3000
  https://www.yokogawa.com/solutions/products-platforms/field-instruments/fiber-optic-sensor/?nid=megadlist
- e-fabDoctor Passport
  e-fabSupport@ml.jp.yokogawa.com

## Keyword:

- Padding Oracle On Downgraded Legacy Encryption Attack (POODLE Attack) : Attack method exploited this vulnerability

## Reference:

1. A Complete Guide to the Common Vulnerability Scoring System (CVSS)
   http://www.first.org/cvss/cvss-guide.pdf
   CVSS is a common language for scoring IT vulnerabilities independent from any vendors. It provides an open framework for communicating the characteristics and impacts of IT vulnerabilities, scaling it in numeric scores.
   The CVSS scores described in this report are provided “AS IS.” Yokogawa has no guarantee over the scores, and the severity caused by the vulnerabilities has to be judged by the users considering the security measures equipped with the overall systems.

2. CERT/CC Vulnerability Note : VU#577193
   http://www.kb.cert.org/vuls/id/577193

## Revision History:

| | |
|---|---|
| December 5, 2014 | 1st Edition |
| December 22, 2017 | 2nd Edition: URLs in Supports are updated. |

* Contents of this document are subject to change without notice.