Yokogawa Security Advisory Report

YSAR-19-0002

Published on May 17, 2019
Last updated on May 17, 2019

YSAR-19-0002: Vulnerability of Microsoft CAPICOM in Yokogawa Products

Overview:

Microsoft CAPICOM (hereafter referred to as “CAPICOM”) * which was ended support by Microsoft has been found to be installed with Yokogawa products. A known vulnerability has been reported in CAPICOM. Yokogawa identified the range of affected products in this report.
Review the report and confirm which products are affected to implement security measures for the overall systems. Also, please consider applying the countermeasures as needed.

* CAPICOM is a Microsoft Cryptographic module.
(Reference: https://en.wikipedia.org/wiki/CAPICOM)

Affected Products:

CAPICOM are installed with the following products.

- CENTUM
  CENTUM VP (R5.02.00 - R6.04.00)
  CENTUM VP Entry Class (R5.02.00 - R6.04.00)
- STARDOM (R3.20 - R4.20)
- B/M9000 VP (R7.02.01 - R8.02.02)

Vulnerability:

Please refer to below URL regarding CAPICOM vulnerability.
https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2007/ms07-028

Countermeasures:

This issue is fixed by CAPICOM file delete. If the file is deleted, the following Yokogawa products operate normally.

Products	Affected Revisions	Countermeasures
CENTUM VP CENTUM VP Entry Class	R5.02.00 - R6.04.00	Please request to delete CAPICOM file to Yokogawa.
STARDOM	R3.20 - R4.20	Please inquire of point of contact for STARDOM. http://stardom.biz/
B/M9000 VP	R7.02.01 - R8.02.02	This product is affected by the existence of CENTUM VP installed on the same PC. Please confirm the above CENTUM VP.

When the CAPICOM file is deleted by Yokogawa personnel, the cost is borne by the customer.

Yokogawa strongly suggest all customers to have a full security program, not only for the vulnerability

identified in this YSAR. Security program components are: Patch updates, Anti-virus, Backup and recovery, zoning, hardening, whitelisting, firewall, etc.

Supports:

For questions related to this report, please contact the below.
https://contact.yokogawa.com/cs/gw?c-id=000498

Reference:

1. Common Vulnerability Scoring System (CVSS)
   https://www.first.org/cvss/
   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.

Revision History:

May 17, 2019 1st Edition

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