

■ INTRODUCTION

This document describes Yokogawa's policy on applying the Microsoft security patches to Yokogawa production control system products. For more information about the overall security policies, refer to the document of "Security Standard of System Product" (TI 33Y01B30-01E).

For strengthening the security of Yokogawa control system products, Yokogawa has setup the following basic policies.

● Segregating Control System Networks

Yokogawa strongly recommends that the control system networks be segregated and a firewall be used to protect the control system networks from the attacks through the other networks.

● Installing Security Patches

Yokogawa understands that the customer's control system may require having similar security countermeasures to a generic Information Technology environment.

Yokogawa monitors Microsoft Security Updates and investigates each in terms of both urgency and impact for Yokogawa products. If the security patch turns out to be relevant to Yokogawa products, Yokogawa will test the security patch on all relevant Yokogawa products to check the instability or if any problem would happen. The importance of each security patch will be webcasted on Yokogawa homepage.

However, installing the security patch to the customers control system should be performed in accordance with the customer's security policy. The impact to the customer's control system needs to be considered in advance and confirmations of system actions need to be performed beforehand.

■ JUDGMENT STANDARD AND PROCESS

Generally, Microsoft releases its security bulletin every month. After Microsoft renews the security bulletin, Yokogawa will perform the following actions.

Step 1

Yokogawa checks the newly released security patch and the affected operating system and applications to determine if the new patch is relevant to the Yokogawa control system products. This check is normally completed within three business days right after Microsoft releasing the new patch. If the new patch is concluded as an irrelevant patch, no further action is required. Go to step 3.

Step 2

Yokogawa performs a test on the relevant control system products with the newly released security patch. This test is targeted to complete within 7 business days right after Microsoft releasing the new patch. The test results, the occurred problems and the countermeasures will be webcasted on Yokogawa homepage.

Step 3

Yokogawa instantaneously updates the information regarding all the security patches on corporate website. The information includes what security patch is relevant to what Yokogawa product and what security patch is irrelevant to Yokogawa products at all.

Step 4

The local Yokogawa service departments will notify the webcasted security information to the customers that contracted with Yokogawa for service support and advice the recommended actions.

Revision Information

Title: Microsoft Security Update Policy
Manual number: TI 33Y01B30-02E

Sep. 2006/1st Edition

Newly published

Sep. 2008/ 2nd Edition

Change in recommendation of security patch

Change the test procedure

Written by Yokogawa Electric Corporation
Published by Yokogawa Electric Corporation
2-9-32 Nakacho, Musashino-shi, Tokyo 180-8750, JAPAN
