

■ Introduction

This document describes Yokogawa's security update policy for Microsoft security patches for Yokogawa standard system products. Refer to TI 33Y01B30-01E Security Standard of System Product.

Concerning measures against threats for PC security, Yokogawa has the following basic policy as documented in the above Technical Information.

● First

It is strongly recommended that the control network segment be entirely segregated from any other segment through a firewall dedicated for access control. It is important for no outside influence be given access to the control system.

● Second

After having segregated the segment, security patches issued by Microsoft should be installed on each PC **only when deemed necessary by Yokogawa**. As many of these security announcements affect applications not authorized to run on Yokogawa control system hardware, not all security patches are required to be installed. Yokogawa investigates each security announcement for applicability to Yokogawa control system and whether each patch is necessary or not.

■ Judgement standards and its process

Microsoft generally publishes its services bulletins the 2nd Tuesday of every month.

Step 1) After a service bulletin is issued by Microsoft, Yokogawa performs the following actions generally within 3 days.

- Evaluate the seriousness of the security threat and determine whether it is "URGENT" to take action or not,
- Evaluate whether the threat can occur without access to a Web site or can occur with any action such clicking an attached file.

If either condition is met, then step 2 is performed. Otherwise, Yokogawa Quality Assurance (QA) will document the Microsoft bulletin number as not necessary in its internal QA tracking system.

Step 2) If the security threat is deemed to be "URGENT", Yokogawa judges the impact of the security bulletin on various Yokogawa products, including systems, productivity solutions and other software that uses Microsoft's operating system. A technical assessment is performed generally within 10 days of the service bulletin announcement based upon whether.

- If the related OS or its revision must be supported or not,
- The type of vulnerability announced and its potential influence on the performance of the system.

If within 10 days after announcement, the technical judgment is that no further action is warranted, Yokogawa will document the Microsoft bulletin number as not necessary in internal QA tracking system.

Step 3) If after step 2, the judgment is that the security patch should be installed, then Yokogawa will verify the security patch with Yokogawa software. The testing and verification is to be finished within 25 days (target time frame) after the Microsoft announcement.

If it is concluded that application of the security patch **is necessary** Yokogawa immediately reports its result and judgment to the related department in Yokogawa. Yokogawa will then document the Microsoft bulletin number as "Required" with the symbol "R" in internal QA tracking system.

Step 4) Yokogawa posts the latest update on the corporate Web site. This is generally updated once per month. All security patches are reported, with an indication of which patches are recommended to be installed highlighted with an "R" next to the security patch and the software product affected.

Step 5) Service departments at Yokogawa local offices will monitor the status of the security patch report, and advise customers who have established service support contracts on recommended actions.