Yokogawa Security Advisory Report

YSAR-18-0002

Published on April 5, 2018
Last updated on April 5, 2018

YSAR-18-0002: Vulnerability of remote management access control on computers provided as Yokogawa system components 2

Overview:

Vulnerability has been found on Intel's hardware-based remote management technologies known as "Intel® Management Engine (ME)" (*). Yokogawa system components affected by this vulnerability are identified in this report.
Review this report and confirm which products in your jurisdiction are affected in order to implement security measures for the overall systems. Also, please consider applying the countermeasures as needed.

*: "ME" is a general term for Remote Management Technology. Sometimes the Remote Management Technology can be called "AMT" according to models.

Affected Products:

Following are the products that would be affected by this vulnerability.
For details, refer to "Countermeasure" described in this document.

No	Classification	Model	Note
1	Global PC	YG1XE2-W0701E YG1T5810-W0701E YG3T330-S0821E	Other Global PC models are out of affected, because AMT configuration of other Global PC models is disabled as initial setting.
2	Selected Equipment	Dell Precision R7610	
3		Dell Precision T3600	YG1T3600-W0701E (Global PC) is not affected by this vulnerability because AMT configuration is disabled as initial setting. If there is "Yokogawa Certified Model" sticker on the PC, it is Global PC
4		Dell Precision T3610	The configuration of T3610 was not standardized by Dell in the global market. It means that T3610 is possibly affected by this vulnerability. Please confirm if AMT is disabled by referring to the countermeasure.

Vulnerability:

Intel published an announcement of an escalation of privilege vulnerability on their AMT's remote management technology.
The affected products on which AMT is enabled are vulnerable to a privilege escalation that allows an unauthenticated attacker to gain access to the remote management features.

CVSS v2 Base Score: 9.0, Temporal Score: 7.4

Access Vector (AV)	Local (L)	Adjacent Network (A)	Network (N)
Access Complexity (AC)	High (H)	Medium (M)	Low (L)
Authentication (Au)	Multiple (M)	Single (S)	None (N)
Confidentiality Impact (C)	None (N)	Partial (P)	Complete (C)
Integrity Impact (I)	None (N)	Partial (P)	Complete (C)
Availability Impact (A)	None (N)	Partial (P)	Complete (C)

Exploitability (E)	Unproven (U)	Proof-of-Concept(POC)	Functional (F)	High (H)	Not Defined (ND)
Remediation Level (RL)	Official Fix (OF)	Temporary Fix (TF)	Workaround (W)	Unavailable (U)	Not Defined (ND)
Report Confidence (RC)	Unconfirmed (UC)	Uncorroborated (UR)	Confirmed (C)	Not Defined (ND)	

Countermeasures:

- YG1XE2-W0701E, YG1T5810-W0701E, Dell Precision R7610, Dell Precision T3600 and T3610
  Disable Intel AMT function in BIOS configuration. (*1)(*2)(*3)(*4)

  *1: Apply this countermeasure without firmware update for all affected products though Dell announced firmware upgrade recommendation.
  *2: After changing ME configuration, it is required to restart the target PC.
  *3: Apply this countermeasure again if BIOS setting is flashed by replacing the motherboard or on-board battery.
  *4: Note: This countermeasure is not needed in case of countermeasure for AMT vulnerability which informed on YSAR-17-0001 has been taken.

- YG3T330-S0821E
  Update BIOS from current version to version 2.3.2.

Countermeasure for each model:

Model	Countermeasure
YG1XE2-W0701E, YG1T5810-W0701E	(1) Calling BIOS setup screen 1.1Restart the target PC. 1.2 Press <Ctrl> + <P> key immediately at the moment of the Dell logo appearance. 1.3 Setup screen “Intel® Management Engine BIOS Extension” appears after “Preparing MEBx menu” message was displayed at the top-right corner of the screen. *Even if “Preparing MEBx menu” message is displayed, there will be no vulnerability on the PC in case of the screen doesn’t shift to “Intel® Management Engine BIOS Extension”. (2) User Authentication 2.1 Select “MEBx Login”, and on the password entry area in the dialog box on the screen, type the password. 2.2 The password is “admin” by default. On the password entry area in the lower part of the screen, type the password. 2.3 In case that it’s the first time to call setup screen, you must change to the new password. * Please appropriately manage the new password by the customer after change. (3) Disable AMT 3.1 Select “Intel® AMT Configuration”, and press <Enter> key. 3.2 Select **“Manageability Feature Selection”**, and press <Enter> key. Note: In case of “Enable”, follow “3.3” procedure to avoid affection of the vulnerability. 3.3 Select **“Disable”** and press <Enter> key. 3.4 After appearing confirmation screen, press <Y> key. (4) Exit setup screen 4.1 Press <Esc> key. 4.2 Select “MEBx Exit”, and press <Enter> key. 4.3 After appearing confirmation screen, press <Y> key. 4.4 The target PC will be restarted automatically.
Dell Precision R7610	(1) Calling BIOS setup screen 1.1Restart the target PC. 1.2 Press <Ctrl> + <P> key immediately at the moment of the Dell logo appearance. 1.3 Setup screen “Intel® Management Engine BIOS Extension” appears. (2) User Authentication 2.1 Select “MEBx Login”, and on the password entry area in the dialog box on the screen, type the password. 2.2 The password is “admin” by default. On the password entry area in the lower part of the screen, type the password. 2.3 In case that it’s the first time to call setup screen, you must change to the new password. * Please appropriately manage the new password by the customer after change. (3) Disable AMT 3.1 Select “Intel® AMT Configuration”, and press <Enter> key. 3.2 Select **“Intel® Standard Manageability Configuration”**, and press <Enter> key. Note: In case of “Enable”, follow “3.3” procedure to avoid affection of the vulnerability. 3.3 Select **“Disable”** and press <Enter> key. 3.4 After appearing confirmation screen, press <Y> key. (4) Exit setup screen 4.1 Press <Esc> key. 4.2 Select “MEBx Exit”, and press <Enter> key. 4.3 After appearing confirmation screen, press <Y> key. 4.4 The target PC will be restarted automatically.
Dell Precision T3600, T3610	(1) Calling BIOS setup screen 1.1Restart the target PC. 1.2 Press <Ctrl> + <P> key immediately at the moment of the Dell logo appearance. 1.3 Setup screen “Intel® Management Engine BIOS Extension” appears. (2) User Authentication 2.1 The password is “admin” by default. On the password entry area in the lower part of the screen, type the password. 2.2 In case that it’s the first time to call setup screen, you must change to the new password. * Please appropriately manage the new password by the customer after change. (3) Disable AMT 3.1 Select “Intel® AMT Configuration”, and press <Enter> key. 3.2 Select **“Manageability Feature Selection”**, and press <Enter> key. 3.3 After appearing confirmation screen, press <Y> key. Note: In case of “Enable”, follow “3.4” procedure to avoid affection of the vulnerability. 3.4 Select **“Disable”** and press <Enter> key.

	(4) Exit setup screen 4.1 Select “Previous Menu”, and press <Enter> key. 4.2 Select “Exit”, and press <Enter> key. 4.3 After appearing confirmation screen, press <Y> key. 4.4 The target PC will be restarted automatically.
YG3T330-S0821E	(1) Updating BIOS 1.1 Download “Update Package for Microsoft® Windows® 64-bit.” on either the following web site. http://www.dell.com/support/home/us/en/04/drivers/driversdetails?driverId=832M2 2.2 Execute the downloaded file.

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

Reference:

1. A Complete Guide to the Common Vulnerability Scoring System (CVSS)
   http://www.first.org/cvss/cvss-v2-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. NIST National Vulnerability Database: CVE-2017-5711, CVE-2017-5712, CVE-2017-5705, CVE-2017-5706, CVE-2017-5707, CVE-2017-5708, CVE-2017-5709, CVE-2017-5710
   https://nvd.nist.gov/vuln/detail/CVE-2017-5711
   https://nvd.nist.gov/vuln/detail/CVE-2017-5712
   https://nvd.nist.gov/vuln/detail/CVE-2017-5705
   https://nvd.nist.gov/vuln/detail/CVE-2017-5706
   https://nvd.nist.gov/vuln/detail/CVE-2017-5707
   https://nvd.nist.gov/vuln/detail/CVE-2017-5708
   https://nvd.nist.gov/vuln/detail/CVE-2017-5709
   https://nvd.nist.gov/vuln/detail/CVE-2017-5710

Revision History:

April 5, 2018 1st Edition

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