Field Safety Notice

SBN-CPS-2018-011

Version 2
24-Sep-2018

Cybersecurity updates in Accu-Chek® Inform II system, cobas h 232 POC system, CoaguChek® Pro II system, CoaguChek® XS Plus / XS Pro systems

Product Name	Accu-Chek® Inform II system CoaguChek Pro II system CoaguChek® XS Plus system CoaguChek® XS Pro system cobas h 232 POC system	
Product Identifier (Product name/Product code)	**Accu-Chek Inform II Instrument**	**05060311001**
	Accu-Chek Inform II Instrument with RF card	**05060303001**
	Accu-Chek Inform II Base Unit	**05060290001**
	Accu-Chek Inform II Base Unit Hub	**05888760001**
	CoaguChek Pro II Kit W-LAN	**07210841190**
	CoaguChek Pro II Kit without W-LAN	07237944190
	CoaguChek XS Plus Kit International	**04800842190**
	CoaguChek XS Pro Kit International	**05530199190**
	cobas h 232 scanner version	**04901142190**
	cobas h 232	**04901126190**
	Handheld Base Unit	**04805658001**
	Note: There may be other affected identifiers that are affected globally. Please contact the product owner if the device is obtained from an overseas dealer. *Only the bold identifiers above are currently supplied in Singapore.*	
Type of Action	Field Safety Corrective Action (FSCA)	

Dear Valued Customer,

We want to inform you about the availability of upcoming cybersecurity updates for the following Roche Diagnostics products Accu-Chek Inform II, cobas h 232, CoaguChek Pro II, CoaguChek XS Plus / XS Pro systems.

Cybersecurity updates in Accu-Chek® Inform II system, cobas h 232 POC system, CoaguChek® Pro II system, CoaguChek® XS Plus / XS Pro systems

Description of Situation

Roche Diagnostics is committed to continuously increase the cyber security of our products. As part of this effort, we plan to release software updates that could further prevent or reduce risk of products being exploited by cyber attackers. Potential risks of cyber-attack include compromised system confidentiality, availability and integrity.

The efforts to perform a successful cyber-attack of our devices were assessed to be highly complex, as attackers with criminal intent would need to physically access, manipulate our devices, or hack into the healthcare network, to successfully exploit potential vulnerabilities. Hence, the likelihood to impact patient safety from such exploitation is assessed to be remote to theoretical.

At the time of the Field Safety Notice, no public exploitation of these security vulnerabilities is known.

Actions taken by Roche Diagnostics

Roche Diagnostics plan to release the following software updates:

Product Code	Product Name	New Software	Date of Release (Global Release Schedule) 2018
05060311001	Accu-Chek Inform II Instrument serial number [redacted]	03.06.00	September
05060303001	Accu-Chek Inform II Instrument with RF serial number [redacted]	03.06.00	September
05060311001	Accu-Chek Inform II Instrument serial number [redacted]	04.03.00	October
05060303001	Accu-Chek Inform II Instrument with RF serial number [redacted]	04.03.00	October
05060290001	Accu-Chek Inform II Base Unit	03.01.04	September
05888760001	Accu-Chek Inform II Base Unit Hub	03.01.04	September
07210841190	CoaguChek Pro II Kit W-LAN	04.03.00	October
07237944190	CoaguChek Pro II Kit without W-LAN	04.03.00	October
04800842190	CoaguChek XS Plus Kit International	03.01.06	September
05530199190	CoaguChek XS Pro Kit International	03.01.06	September
04901142190	**cobas h** 232 Kit (scanner) with serial number [redacted]	03.01.03	October
04901126190	**cobas h** 232 with serial number [redacted]	03.01.03	October
04901142190	**cobas h** 232 Kit (scanner) with serial number [redacted]	04.00.04	October
04901126190	**cobas h** 232 with serial number [redacted]	04.00.04	October
04805658001	Handheld Base Unit	03.01.04	September

Cybersecurity updates in Accu-Chek® Inform II system, cobas h 232 POC system, CoaguChek® Pro II system, CoaguChek® XS Plus / XS Pro systems

Actions to be taken by the customer/user

Medical device cybersecurity is a shared responsibility among multiple stakeholders including health care facilities, providers, and manufacturers.

Roche Diagnostics recommends an update of your device software to further improve the cyber security of the device once available, according to the table above. Since the likelihood to impact patient safety from such exploitation is assessed to be remote to theoretical an update to your device is **not mandatory**.

In general, Roche Diagnostics would like to remind you to put the following measures in place to increase your cyber security (if in case still not implemented):

For connected devices (Ethernet and Wi-Fi):

- Restrict network and physical access to the device and attached infrastructure by enabling the device security features
- Protect connected endpoints from unauthorized access, theft and malicious software
- Monitor the system and network infrastructure for suspicious activity and report a suspected compromise according to your local policy

For non-connected devices:

- Protect from unauthorized access, theft and manipulation

Please contact your local Roche Diagnostics office if you have any further questions or concerns (contact details below).

Cybersecurity updates in Accu-Chek® Inform II system, cobas h 232 POC system, CoaguChek® Pro II system, CoaguChek® XS Plus / XS Pro systems

Communication of this Field Safety Notice

This notice must be passed on to all those who need to be aware within your organization or to any other organization/individual where the potentially affected devices have been distributed/supplied. Please pass on this notice to the Chairman Medical Board and Head of Department as well, as required by HSA.

Please maintain awareness of this notice and resulting action for an appropriate period to ensure the effectiveness of the corrective action

We apologize for any inconvenience this may cause and hope for your understanding and your support.

Sincerely,

Roche Diagnostics Asia Pacific Pte Ltd
Email: sg.regulatory@roche.com