Urgent: Notification : Medical Device Security Update

Date: September 10, 2021

Product Field Action number : PR 2795031

Microsoft Windows Print Spooler Vulnerabilities

Attn: IT/Security Manager, Materials Manager, OR Manager

Dear Customer,

Issue description

Microsoft has issued a notification of vulnerabilities related to the Windows Print Spooler service, including CVE-2021-34527 and CVE-2021-36958.

To date, Stryker has received no reports of impact on Stryker Instruments products related to these vulnerabilities. Applicable product portfolios were assessed against these vulnerabilities; the products identified below were found to be potentially exploitable.

Product	Description	GTIN	Affected units
7700-600-000	ADAPT Platform	04546540696410	All units manufactured in 2012 to present
7700-700-000	Nav3 Platform	04546540696427	
7700-800-000	NAV3i Platform	07613327004175	
8000-010-003	Scopis Electromagnetic Navigation Unit	07613327413083	
7700-009-100	NavSuite 3 Kit	07613327114782	
7700-009-102	NavSuite 3 Upgrade Kit	07613327114973	

Risk to health

Microsoft has classified this vulnerability as critical and has disclosed that exploitation has occurred globally. However, upon investigation of the Stryker products listed above, Stryker has determined that exploitation is very unlikely. In the unlikely event of an exploit, an attacker could potentially gain access to patient data, restrict access, or stop navigation before or during a surgical procedure.

As a general reminder, it is recommended these devices should be disconnected from the network prior to any navigation usage during a surgical procedure.

Actions to be taken

Stryker representative and technical support are equipped to perform Microsoft's recommendations to avoid any potential exploitation.

1. Please contact your local Stryker sales representative or technical support for assistance.
2. Once the applicable defensive measures are implemented, complete and sign this notification, acknowledging your organization's awareness of these vulnerabilities.
3. Email this signed form to asean.pms@stryker.com
4. Maintain awareness of this communication internally.

(Turn over for page 2)

For IT/Security Managers needing further information, please go to:
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527.

Important terms & definitions

Vulnerable: Per Microsoft, vulnerability is a security exposure that results from a product weakness that the product developer did not intend to introduce and should fix once it is discovered.

Exploitable: Per Microsoft, exploitable code is a software program or sample code that, when executed against a vulnerable system, uses the vulnerability to spoof attacker identity, tamper with user or system information, repudiate attacker action, disclose user or system informationon the server side, deny service to valid users, or elevate privileges for the attacker.

On behalf of Stryker we thank you sincerely for your help and support in completing this action.

Sincerely,

Chia Nee Lim
Chia Nee Lim
Senior QA Specialist
chianee.lim@stryker.com
ASEAN.PMS@stryker.com
+65 6662 5905

Urgent: Notification : Medical Device Security Update

Business Reply Form

Product Field Action number : PR 2795031

Date: 10 Sept 2021

Dear Customer,

Please complete the Business Reply Form within 5 business days and email a copy to ASEAN.PMS@stryker.com.

Note: Your signature below indicates you have received and understand this notification and that you have taken the necessary applicable defensive measures on all affected products at your facility.

Facility Name			
Form Completed by (Printed Name)		**Title**	
Signature		**Phone**	
Date		**Email**	
If products were further distributed to another facility			
Product Name		**Quantity Distributed**	
Facility Name		**Contact Person**	