

🌐 Select Country / Region

(<https://global.medtronic.com/xg-en/index.html>)
PACEART OPTIMA SYSTEM APPLICATION SECURITY UPDATE



June 29, 2023

SUMMARY

Medtronic has identified a vulnerability in an optional messaging feature in the Paceart Optima cardiac device data workflow system. This feature is not configured by default, and it cannot be exploited unless enabled. As a precautionary measure, Medtronic is notifying customers that if exploited, this vulnerability could result in a healthcare delivery organization's Paceart Optima system's cardiac device data being deleted, stolen, or modified, or the Paceart Optima system being used for further network penetration.

Healthcare delivery organizations should work with Medtronic Paceart technical support to install an update to the Paceart Optima application to eliminate this vulnerability from the Paceart Application Server. This security bulletin also includes immediate, temporary steps for a healthcare delivery organization to take to prevent the exploitation of this vulnerability.

PRODUCTS IMPACTED

Paceart Optima™ is a software application that runs on a healthcare delivery organization's Windows server. The application collects, stores, and retrieves cardiac device data from programmers and remote monitoring systems from all major cardiac device manufacturers to aid in standard workflows. The Paceart Optima product consists of multiple components that work together to deliver product functionality. This vulnerability impacts the Application Server component.

Versions affected:

- Paceart Optima application versions 1.11 and earlier

VULNERABILITY OVERVIEW

At this time, Medtronic has not observed any cyberattacks, unauthorized access to or loss of patient data, or harm to patients related to this issue.

During routine monitoring, Medtronic identified a vulnerability in the optional Paceart Messaging Service within the Paceart Optima system, specifically in the Paceart Messaging Service's implementation of the Microsoft Message Queuing Protocol. The Paceart Messaging Service

enables healthcare delivery organizations to send fax, email, and pager messages within the Paceart Optima system.

If a healthcare delivery organization has enabled the optional Paceart Messaging Service in the Paceart Optima system, an unauthorized user could exploit this vulnerability to perform Remote Code Execution (RCE) and/or Denial of Service (DoS) attacks by sending specially crafted messages to the Paceart Optima system. RCE could result in the Paceart Optima system's cardiac device data being deleted, stolen, or modified, or the Paceart Optima system being used for further network penetration. A DoS attack could cause the Paceart Optima system to become slow or unresponsive.

The vulnerability is present in Paceart Optima system versions 1.11 and earlier.

RECOMMENDED ACTIONS

IMMEDIATE MITIGATION ACTIONS:

If you have a combined Application and Integration Server, contact Medtronic Paceart Optima system technical support for immediate mitigation actions. All other configurations, follow the steps below.

The vulnerable code will still be present in the application, but will no longer be exploitable.

Step 1: Manually disable the Paceart Messaging Service on the Application Server.

1. Open the 'Windows Services' application
2. Find the 'Paceart Messaging Service'
3. Right-click the 'Paceart Messaging Service' and select 'Properties'
4. Select 'Stop' to stop running the service and change the startup type to 'Disabled'
5. Select 'Apply'

Step 2: Manually disable message queuing on the Application Server.

1. Open server manager
2. Select 'Add roles and features'
3. Select 'Start the Remove Roles and Features Wizard'
4. Before you begin – next
5. Server selection – next
6. Server roles – next
7. Features section – take action. Select the black box next to Message Queuing
8. When the window pops up select 'Remove Features' button
9. Select 'next'
10. Confirmation – select 'Remove'

As long as the Paceart Messaging Service remains disabled, the vulnerability will remain mitigated.

LONG-TERM REMEDIATION ACTION:

For a complete mitigation on the Application Server, update the Paceart Optima system to version 1.12. This update removes the Paceart Messaging Service function and fully remediates the vulnerability on the Application Server. To schedule an update, please reach out to dl.paceartupdate@medtronic.com (<mailto:dl.paceartupdate@medtronic.com>).

If you are a patient and are concerned about care delivery associated with the Paceart Optima system, please consult your care provider.

FOR MORE INFORMATION:

Contact for more support: Medtronic Paceart Optima system technical support
1-800-PACEART (722-3278)

ADDITIONAL DETAILS:

Cybersecurity professionals may find the following technical information useful for tracking and risk rating purposes:

- The vulnerability has been assigned a CVE number, CVE-2023-31222
 - The CVSS score for this vulnerability is 9.8.
-

DEFINITIONS:

Remote Code Execution – Remote code execution (RCE) is a type of security vulnerability that allows attackers to run arbitrary code on a remote machine if connected to it.
([name=%22remote%22](#))

Denial of Service Attack - A DoS is a type of cyberattack that is meant to shut down a machine, function or network, making it inaccessible to its intended users by consuming available resources with invalid activity. The most common DoS technique is to send invalid network requests that consume available network resources of an online service.

Exploit -An exploit is a program or methodology created to take advantage of a vulnerability in a system or product to gain unauthorized access or negatively affect proper operation.

Vulnerability - A vulnerability is a weakness in systems, software or products that compromises security. A vulnerability allows people to perform bad actions on those same systems, software and products.

Translation

To translate this bulletin into your native language, use your browser's translation function. Please refer to your browser's help section for more information.

OPT-IN TO RECEIVE BULLETINS

[SIGN UP \(https://global.medtronic.com/xg-en/product-security/security-bulletins/register.html\)](https://global.medtronic.com/xg-en/product-security/security-bulletins/register.html)



(mailto:?



body=https%3A%2F%2Fglobal.m
edtronic.com%2Fzg-
en%2Fproduct-
security%2Fsecurity-
bulletins%2Fpaceart-optima-
system.html)

Disclaimer: This page may include information about products that may not be available in your region or country. Please consult the approved indications for use. Content on specific Medtronic products is not intended for users in markets that do not have authorization for use.



[Our Company \(https://global.medtronic.com/xg-en/our-company.html\)](https://global.medtronic.com/xg-en/our-company.html)

[Careers \(https://global.medtronic.com/xg-en/our-company/careers.html\)](https://global.medtronic.com/xg-en/our-company/careers.html)

[Contact & Support \(https://www.medtronic.com/us-en/about/contact-us.html\)](https://www.medtronic.com/us-en/about/contact-us.html)

[Locations \(https://global.medtronic.com/xg-en/our-company/locations.html\)](https://global.medtronic.com/xg-en/our-company/locations.html)

[ID Cards \(https://global.medtronic.com/xg-en/patients/update-device-registration.html\)](https://global.medtronic.com/xg-en/patients/update-device-registration.html)

[Order Products\(opens new window\) \(https://americas.connect.medtronic.com/apps/portal/login\)](https://americas.connect.medtronic.com/apps/portal/login)

[Diabetes Supplies\(opens new window\) \(https://www.diabetes.shop/\)](https://www.diabetes.shop/)

[MRI Tools \(https://global.medtronic.com/xg-en/patients/mri-access.html\)](https://global.medtronic.com/xg-en/patients/mri-access.html)

[Recycling \(https://global.medtronic.com/xg-en/healthcare-professionals/products/product-stewardship/product-packaging-disposition.html\)](https://global.medtronic.com/xg-en/healthcare-professionals/products/product-stewardship/product-packaging-disposition.html)

[Product Manuals\(opens new window\) \(https://manuals.medtronic.com/manuals/main/region\)](https://manuals.medtronic.com/manuals/main/region)

[Product Security \(https://global.medtronic.com/xg-en/product-security.html\)](https://global.medtronic.com/xg-en/product-security.html)

[Electromagnetic Compatibility for Cardiac Devices \(https://global.medtronic.com/xg-en/patients/electromagnetic-guide.html\)](https://global.medtronic.com/xg-en/patients/electromagnetic-guide.html)

[California Transparency in Supply Chains Act \(https://www.medtronic.com/us-en/about/corporate-governance/suppliers/supplier-standards-policies/ca-transparency-act.html\)](https://www.medtronic.com/us-en/about/corporate-governance/suppliers/supplier-standards-policies/ca-transparency-act.html)

[Information About Proposition 65 for California Customers \(https://www.medtronic.com/us-en/about/corporate-governance/ca-proposition-65.html\)](https://www.medtronic.com/us-en/about/corporate-governance/ca-proposition-65.html)

[Digital Millennium Copyright Act \(DMCA\) Notification \(/xg-en/about/corporate-governance/dmca-notification.html\)](/xg-en/about/corporate-governance/dmca-notification.html)

[Privacy Statement \(/xg-en/privacy-statement.html\)](/xg-en/privacy-statement.html)

[Accessibility Statement \(/xg-en/privacy-statement/accessibility-statement.html\)](/xg-en/privacy-statement/accessibility-statement.html)

[Terms of Use \(/xg-en/terms-of-use.html\)](/xg-en/terms-of-use.html)

Medtronic Operational Headquarters 710 Medtronic Parkway Minneapolis, MN 55432-5640 USA

Last Updated June 2023 © 2023 Medtronic