Drägerwerk AG & Co.KGaA, 23542 Lübeck

Our reference
PSA-24-183-2

Vulnerability and Incident Reporting
product-security@draeger.com

# Dräger Product Security Advisory PSA-24-183-2

Vista 120 CMS Security Vulnerabilities

**Legal Notice**

This Product Security Advisory is based on all our findings that we had at the time of publication. However, the facts of the case are being reviewed on an ongoing basis and it is possible that this may result in changed assessments or that assessments contained in this advisory may turn out to be incorrect. We also reserve the right to change or revoke any recommendations. In addition, differences may result from the circumstances of the individual case on site. This information is naturally not available to us and has not been taken into account. Dräger can therefore accept no responsibility that the information presented here is conclusive or comprehensively correct for you. Therefore, please check carefully to what extent deviations can arise for your individual case. If necessary, you will be informed about new findings through following advisories.

## 1. Publication Date

2024-07-01 (updated 2024-08-16)

## 2. Overview

CVE-2023-43208 states that NextGen Mirth Connect before version 4.4.1 is vulnerable to unauthenticated remote code execution. Mirth Connect is installed as part of the Dräger product Vista 120 CMS.
The full text of this advisory can be accessed through https://static.draeger.com/security.

## 3. Affected Products

The following Dräger products are affected by this vulnerability:

- Vista 120 CMS from version 1.6 to 1.64.02

## 4. How to verify if the product is affected

NextGen Mirth Connect is installed as an optional component (installed separately) for the affected Vista 120 CMS versions. The server, however, is not operational until Dräger Service activates the connection. Only installations of Vista 120 CMS where Next Gen Mirth Connect is enabled are vulnerable.

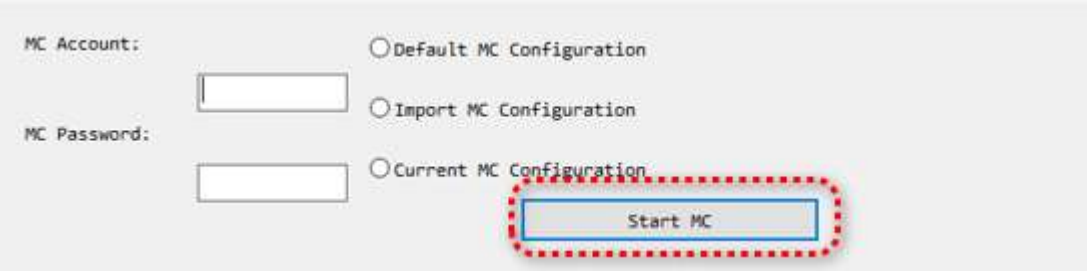
The steps to Identify which version of Vista 120 CMS you are using are as follows:

1. Navigate to the Vista 120 CMS interface.
2. Click on the User Maintain tab, input the Password, then click OK.
3. Click on About on the left tree control and check the Full Version.

If your CMS version is in the affected range, please proceed further to identify if you are using NextGen Mirth Connect:

1. Navigate to the Vista 120 CMS interface.
2. Click on Factory Maintain tab, input the Password (Dräger Service Password), then click OK.
3. Click on Mirth Connect (MC) on the left tree control, check if the NextGen Mirth Connect is started or not.
4.

If “Start MC” is shown, your Vista 120 CMS instance is **NOT** impacted, as it does **NOT** use Mirth.




If Stop MC is shown, your Vista 120 CMS instance is impacted and the ***Error! Reference source not found.*** steps below are advised.

Use of this document / contents is forbidden without express authority. All rights reserved. Refer to protection notice ISO 16016.
Printed copies are uncontrolled and for reference purposes only.




## 5. Vulnerability Description

The vulnerability was discovered following an incomplete patch to CVE-2023-37679. Research by Horizon3.ai revealed a bypass to the deny list implemented in the original patch, leading to the identification of CVE-2023-43208. This exploit module has been successfully tested against Mirth Connect versions 4.1.1, 4.3.0, and 4.4.0. [1]
This is an easily exploitable, unauthenticated remote code execution vulnerability. Attackers would most likely exploit this vulnerability for initial access or to compromise sensitive healthcare data. [2]
A proof of concept has been published [3].

## 6. Impact

In the event of successful exploitation, the vulnerability allows an attacker to remotely execute arbitrary commands in NextGen Mirth Connect on the hosting server. Depending on the privileges under which Mirth Connect had been installed, a successful attacker can potentially access all data on that system or use that system as a vantage point to further explore the local network.

## 7. Severity

The computed CVSS 3.1 scores are as follows:

| | |
|---|---|
| Base Score: | 9.8 |
| Severity: | Critical |
| Vector: | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H |

## 8. Mitigation/Remediation

Customers using an affected version of Vista 120 CMS should contact Dräger Service to schedule the installation of an updated version of Vista 120 CMS (version 1.64.03 or later).
Based on their own IT network risk assessment customers may choose to disable the vulnerable component Mirth Connect until the patched version is installed by following the steps outlined in section 4 of this document.

## 9. Contact Information

If you have any further questions related to the impact of the vulnerabilities, please contact your designated regional marketing manager. For reporting incidents and potential vulnerabilities in our devices, please refer to https://static.draeger.com/security to contact the Product Security team directly.

Use of this document / contents is forbidden without express authority. All rights reserved. Refer to protection notice ISO 16016.
Printed copies are uncontrolled and for reference purposes only.

## 10. References

[1] Health-ISAC Alerts
[2] NextGen Mirth Connect Remote Code Execution Vulnerability (CVE-2023-43208) – Horizon3.ai
[3] Writeup for CVE-2023-43208: NextGen Mirth Connect Pre-Auth RCE – Horizon3.ai

## 11. Change log

| Version | Date | Comments |
|---|---|---|
| 1.0 | 2024-07-01 | PSA-24-183-1: Initial Advisory |
| 1.1 | 2024-08-16 | PSA-24-183-2: Revised the mitigation/remediation section to include the CMS software version introducing the fix |

Use of this document / contents is forbidden without express authority. All rights reserved. Refer to protection notice ISO 16016.
Printed copies are uncontrolled and for reference purposes only.