Dräger Product Security Advisory PSA-21-120-1

Dräger X-Dock 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

2021-04-30

2   Overview

Security Vulnerabilities have been identified in the X-Dock Firmware. The vulnerabilities can lead to an attacker being able to get root access to the underlying operating system.

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:

- Dräger X-Dock Firmware versions prior to and excluding 03.00.13.

4   How to verify if the product is affected

Open the information screen on the device to review the software version. The software version is also displayed on the screen during device startup.

5   Vulnerability Description

Use of Hard-Coded Credentials (CWE-798)
CVE-2021-28111

Active Debug Code (CWE-489)
CVE-2021-28112

An unused debug port with hard coded credentials was identified on the system.

6   Impact

By extracting and using the hard coded credentials an authenticated remote attacker is able to execute arbitrary code on the system.

7   Severity

The vulnerability can only be exploited in conjunction of CVE-2021-28111 and CVE-2021-28112, therefore, a combined CVSS score is being calculated.

CVSS 3.1 Score

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

8   Remediation

The software has been patched to mitigate the vulnerability. Customers are urged to install the fixed versions as soon as possible:

- Dräger X-Dock Firmware versions 03.00.13 and later.

In the meantime, customers are advised to disconnect the network connection to devices running affected firmware versions. If data export is needed, customers are advised to use USB export in the meantime (mobile sync).

9   Credit

Dräger would like to thank the ZDI for finding and reporting these vulnerabilities to us!

10   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.

11   Revision History

VERSION	DATE	COMMENTS
1.0	2021-04-30	Initial Advisory