

TRAKA PRODUCT SECURITY ADVISORY

LANTRONIX DEVICE SERVERS (CVE-2025-2567)

Document ID	Date	Revision	Initial publication	Document category
Traka-PSA-2025-01	16/05/2025	1.0	27/05/2025	Information

TLP:WHITE

No restriction on distribution

OVERVIEW

Traka has been informed about a vulnerability report, [CVE-2025-2567](#) and initially identified in [icsa-25-105-05](#), concerning Lantronix XPort and UDS2100 device servers. This issue impacts the following Traka solutions that use these devices:

- First-generation Key Management with separate keypad and LCD
- First-generation Equipment Management (Lockers) with separate keypad and LCD
- First-generation Access Control Equipment with separate keypad and LCD systems

These are commonly referred to as Traka 8-bit and 16-bit systems.

The vulnerability is discussed on the Lantronix website: [CVE-2025-2567 Lantronix XPort Missing Authentication for Critical Function vulnerability](#)

The critical vulnerability scoring system (CVSS) has rated this as a critical vulnerability with a rating of 9.3 and we therefore recommend immediate remedial action.

NEXT STEPS

The following products are in scope of this vulnerability announcement.

Traka 8-bit and 16-bit systems, regardless of connected software platform, meeting the following criteria:

- Fitted with **Lantronix XPort-03, XPort-04, XPort-05** - a component fitted to the 8-bit/16-bit control board, accessible behind the system's front panel.
- Fitted with **Lantronix UDS2100** – connected externally to the **8-bit/16-bit control board** but typically located behind the Traka system's front panel. UDS2100 is used for Traka32 with TACLS/RTUS (Real Time Update) scenarios.

If you are unsure, please contact Traka Technical Support.

It is important to note that the remediation process differs depending upon the Lantronix Device Server identified.

For Traka systems with a Lantronix XPort-05 or Lantronix UDS2100 fitted to the control board, Lantronix have released a firmware update which can be obtained from the Lantronix website, but we recommend that you follow the below documented steps in context of Traka products.

For Traka systems fitted with a Lantronix XPort-03 or XPort-04 device server, at the time of writing, there is no firmware available to mitigate the identified vulnerability. However, Lantronix have issued guidance to provide mitigations, also covered in the below document.

For information on how to identify the specific device servers, how to mitigate the vulnerability for each component and additional resources, please read "TD0226 - CVE- 2025-2567 remediation guide for Lantronix Device Servers". Document TD0226 is available to customers with active support contracts and a support site login at <https://support.traka.com/>. If you don't have a login for our support website, then please contact your local Traka Technical Support for assistance.

CONTACT INFORMATION

If you have additional questions, please contact your local Traka technical support.

REFERENCES

Source	Location
Lantronix article on CVE-2025-2567	https://ltrxdev.atlassian.net/wiki/spaces/LTRXTS/pages/3130916865/CVE-2025-2567+Lantronix+XPort+Missing+Authentication+for+Critical+Function+vulnerability
Traka Remediation Technical Document	The below document can be obtained from the Traka Support site at https://support.traka.com/ TD0226 - CVE- 2025-2567 remediation guide for Lantronix Device Servers
NIST Vulnerability Database - CVE	https://nvd.nist.gov/vuln/detail/CVE-2025-2567
CISA ICS Advisory	https://www.cisa.gov/news-events/ics-advisories/icsa-25-105-05

TERMS OF USE

THIS DOCUMENT IS PROVIDED "AS IS". IT DOES NOT IMPLY ANY KIND OF GUARANTEE, WARRANTY, OR UNDERTAKING, NOR DOES IT EXPAND THE SCOPE OF ANY GUARANTEE, WARRANTY OR UNDERTAKING MADE IN ANY AGREEMENT TO WHICH AN ASSA ABLOY GROUP COMPANY IS A PARTY, INCLUDING THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. ANY USE OF THE INFORMATION CONTAINED HEREIN OR MATERIALS LINKED FROM THIS DOCUMENT IS AT YOUR OWN RISK. ASSA ABLOY GLOBAL SOLUTIONS RESERVES THE RIGHT TO CHANGE OR UPDATE THIS DOCUMENT AT ANY TIME.

A STANDALONE COPY OR PARAPHRASE OF THE TEXT OF THIS DOCUMENT THAT OMITTS THE DISTRIBUTION URL IS AN UNCONTROLLED COPY. UNCONTROLLED COPIES MAY LACK IMPORTANT INFORMATION OR CONTAIN FACTUAL ERRORS. THE INFORMATION IN THIS DOCUMENT IS INTENDED SOLY FOR END USERS' LAWFUL USE OF ASSA ABLOY GLOBAL SOLUTIONS PRODUCTS.