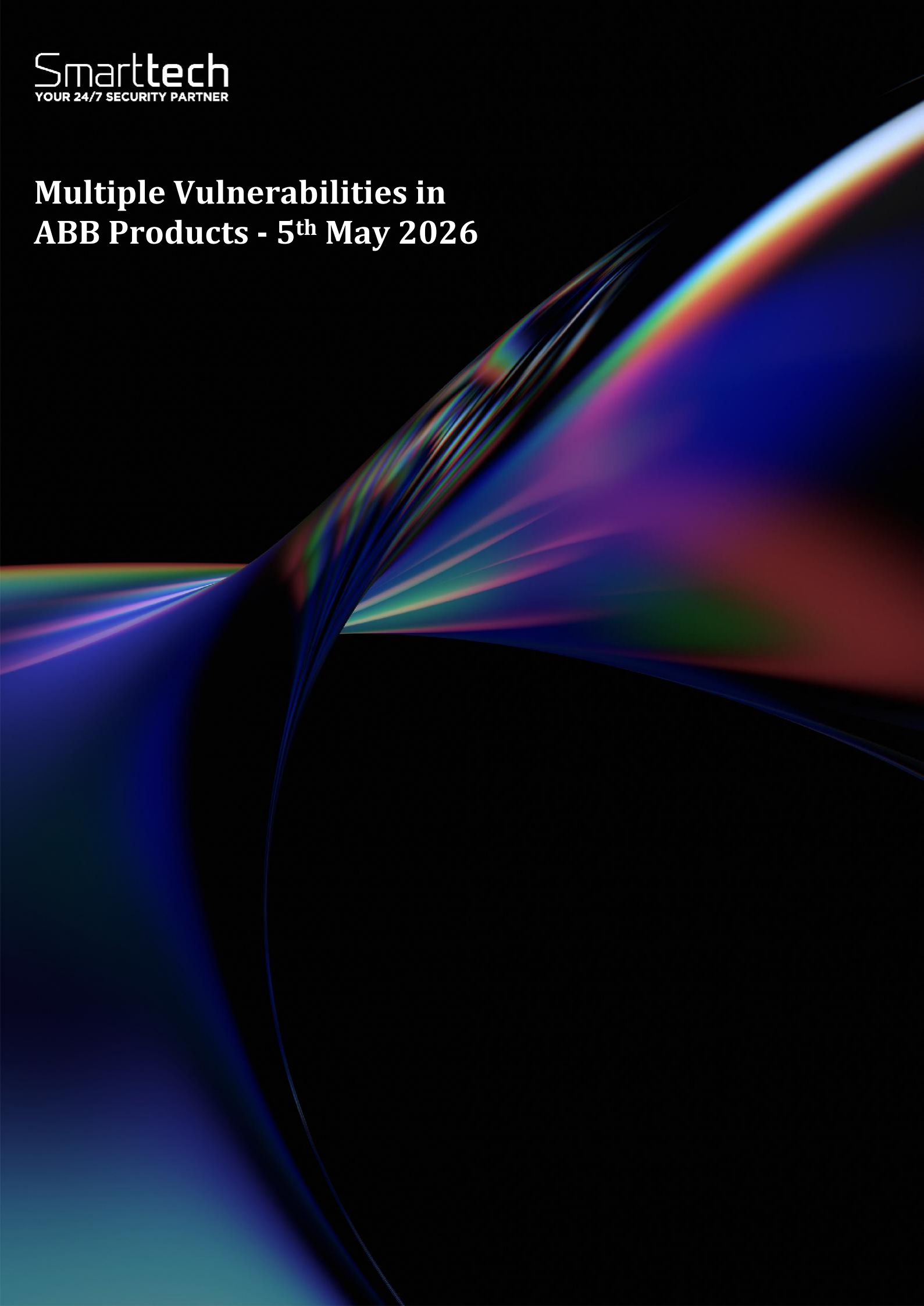
Smarttech
YOUR 24/7 SECURITY PARTNER

# Multiple Vulnerabilities in ABB Products - 5th May 2026



| | |
|---|---|
| **Document ID** | SMA-Threat Report |
| **Document status** | ISSUED |
| **Issue Number** | 61 |
| **Authors** | Alex Ciuta < alexandru.ciuta@smarttech247.com > |
| **Verified by** | Alin Curcan < alin.curcan@smarttech247.com > |
| **Last modified** | 2026-05-05 |
| **Issue Date** | 2026-05-05 |

**Threat Reports** are reports created by Smarttech247 based on high and critical severity vulnerabilities that may have a high potential to be exploited in the wild i.e. vulnerabilities that are present in most used products by companies and do not have an auto-update option or they are usually not automatically updated in case that could lead to some service disruption. This report is usually created as soon as the vulnerability is released, therefore we strongly recommend that the information is reviewed, tests are performed and patches are applied before the first proof-of-concept is released.
Even though certain vulnerabilities may not have an active exploit in the wild at the time that we report on them, we take into consideration the wider risk and the impact it could have on systems, should an exploit like that be available after a while. Our duty is to report them on time and we recommend enterprises that, in order to keep critical business systems protected, they should consider, on average, ten working days to check whether or not the new vulnerability affects them, and if so, to implement actions in order to remove the risk.

## Overview

Multiple vulnerabilities have been identified in the following Industrial Control Systems / ICS-connected products: **ABB System 800xA, Symphony Plus IEC 61850, ABB PCM600, ABB Edgenius Management Portal, ABB Ability OPTIMAX, ABB AWIN Gateways** and **ABB Ability Symphony Plus Engineering.** Successful exploitation of these vulnerabilities across the affected ABB products could enable attackers to execute arbitrary code, compromise system nodes, modify or uninstall applications, bypass authentication mechanisms such as Azure Active Directory Single Sign-On, remotely reboot devices, access sensitive configuration details through unauthenticated queries, and ultimately gain unauthorized control over engineering environments—particularly where PostgreSQL 13.11 and earlier versions are embedded—potentially leading to full system compromise if an attacker obtains access to the S+ Client Server network.

## ABB System 800xA, Symphony Plus IEC 61850

### Summary

This vulnerability was privately reported relating to ABB's implementation of the IEC 61850 communication stack for MMS client applications used in some Automation control system products.

The following versions of ABB System 800xA, Symphony Plus IEC 61850 are affected:

- **AC800M Product line (System 800xA) CI868**
- **Symphony Plus SD Series CI850**
- **Symphony Plus MR (Melody Rack) PM 877**
- **S+ Operations**
- **Firmware <=6.0.0303.0, <=6.1.0031.0 , <=6.1.1004.0 , <=6.1.1202.0 , <=6.2.0006.0 , 6.1.1-3, 7.0, A_0, A_1, A_2.003, A_3.005, A_4.001, B_0.005, C_0, >=3.10|<=3.52, 3.53, 3.3, 2.3, 2.2, 2.1, 3.4 ()**

- **CVSS v.3** 6.5
- **Vendor:** ABB
- **Equipment:** AC800M Product line (System 800xA) CI868
- **Vulnerabilities:** AC800M Product line (System 800xA) CI868

### Vulnerabilities

| CVE ID | Base Severity | Description |
|---|---|---|
| **CVE-2025-3756** | Medium | A vulnerability exists in the command handling of the IEC 61850 communication stack included in the product revisions listed above. An attacker with access to IEC 61850 networks could exploit the vulnerability by using a specially crafted 61850 packet, forcing the communication interfaces of the PM 877, CI850 and CI868 modules into fault mode or causing unavailability of the S+ Operations 61850 connectivity, resulting in a denial-of-service situation. The System 800xA IEC61850 Connect is not affected. Note: This vulnerability does not impact on the overall availability and functionality of the S+ Operations node, only the 61850 communication function. |

**Remediation:** ABB advises all customers to review their installations to determine if they are using an impacted product as listed above, no further analysis or tools are needed to make this determination. The recommended immediate actions per product are listed below: - CI868 (for AC 800M) Devices with firmware versions reported in Affected products are vulnerable. All the vulnerabilities will be corrected in 6.1.1 and 7.0 tracks for 800xA. AC 800M 6.1.1-3 is planned for Q2 2027, AC 800M 7.0 has been released in December 2025. - CI850 (for Symphony Plus SD Series) Devices with firmware versions reported in Affected products are vulnerable. All the vulnerabilities will be corrected in version C_0 or later (planned Q2 2026). - PM 877 (Symphony Plus MR) Devices with firmware versions reported in Affected products are vulnerable. All the vulnerabilities will be corrected with firmware version 3.53 or later (planned Q1 2026). - S+ Operations Versions reported in Affected products are vulnerable. All the vulnerabilities will be corrected in version 3.4 or later (released in January 2026). ABB recommends customers apply updates, as they become available, at their earliest convenience. It is also advisable to review the Mitigating Factors, Workarounds and General security recommendations sections for additional actions which may help reduce overall risk.

## ABB PCM600

### Summary

Successful exploitation of this vulnerability could allow an attacker to send specially crafted messages to the system node resulting in execution of arbitrary code.

The following versions of ABB PCM600 are affected:

- **PCM600 >=1.5|<=2.13**

- **CVSS v3 4.4**
- **Vendor: ABB**
- **Equipment: ABB PCM600**
- **Vulnerabilities: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')**

**Vulnerabilities**

| CVE ID | Base Severity | Description |
|---|---|---|
| **CVE-2018-1002208** | Medium | A vulnerability exists in the SharpZip.dll included in the product versions listed above. An attacker could exploit vulnerability by providing a specially crafted message to the system node, causing insertion, and running of arbitrary code. |

**Remediations:** The problem is corrected in the following product version: ABB Protection and control IED manager PCM600 version 2.14. ABB recommends that customers apply the update at earliest convenience.

## ABB Edgenius Management Portal

**Summary**

Successful exploitation of this vulnerability could allow an attacker to send a specially crafted message to the system node allowing the attacker to install and run arbitrary code, uninstall applications, and modify the configuration of installed applications.

The following versions of ABB Edgenius Management Portal are affected:

- **Edgenius Management Portal 3.2.0.0|3.2.1.1**

- **CVSS v3 9.6**
- **Vendor: ABB**
- **Equipment: ABB Edgenius Management Portal**
- **Vulnerabilities: Authentication Bypass Using an Alternate Path or Channel**

**Vulnerabilities**

| CVE ID | Base Severity | Description |
|---|---|---|
| **CVE-2025-10571** | Critical | The Edgenius Management Portal in the affected product versions contains a vulnerability that allows authentication to be bypassed. An attacker could exploit the vulnerability by sending a specially crafted message to the system node allowing the attacker to install and run arbitrary code, uninstall in-stalled applications and modify the configuration of installed applications. |

**Remediations:**
ABB has prepared an update to fix this vulnerability included in the latest Roll-Up, ABB Ability Edgenius version 3.2.2.0. ABB advises customers to upgrade as soon as possible. Until the upgrade is applied, ABB advises customers to disable the Edgenius Management Portal to mitigate the vulnerability.

**Mitigation:**
Ability Edgenius 3.2.2.0 is a fixed version for CVE-2025-10571

## ABB Ability OPTIMAX

### Summary

Successful exploitation of this vulnerability could allow an attacker to bypass user authentication on OPTIMAX installations that make use of the Azure Active Directory Single-Sign On integration.

The following versions of ABB Ability OPTIMAX are affected:

- **ABB Ability OPTIMAX 6.1 vers:all/***
- **ABB Ability OPTIMAX 6.2 vers:all/***
- **ABB Ability OPTIMAX 6.3 <6.3.1-251120**
- **ABB Ability OPTIMAX 6.4 <6.4.1-251120**

- **CVSS v3 8.1**
- **Vendor: ABB**
- **Equipment: ABB Ability OPTIMAX**
- **Vulnerabilities:** Incorrect Implementation of Authentication Algorithm

### Vulnerabilities

| CVE ID | Base Severity | Description |
|---|---|---|
| **CVE-2025-14510** | High | The vulnerability allows an attacker to bypass user authentication on OPTIMAX installations that make use of the Azure Active Directory Single-Sign On integration. |

**Remediations:**
Ability OPTIMAX 6.3 6.3.1-251120 is a fixed version for CVE-2025-14510

## ABB AWIN Gateways

### Summary

Successful exploitation of these vulnerabilities could allow an attacker to remotely reboot the device or complete an unauthenticated query to reveal system configuration, including sensitive details.

The following versions of ABB AWIN Gateways are affected:

- **ABB AWIN Firmware (2.0-0) installed on ABB AWIN GW100 rev.2 2.0-0**
- **ABB AWIN Firmware (2.0-1) installed on ABB AWIN GW100 rev.2 2.0-1**
- **ABB AWIN Firmware (1.2-0) installed on ABB AWIN GW120 1.2-0**
- **ABB AWIN Firmware (1.2-1) installed on ABB AWIN GW120 1.2-1**

- **CVSS v3 8.3**
- **Vendor: ABB**
- **Equipment: ABB AWIN Gateways**
- **Vulnerabilities: Authentication Bypass by Capture-replay, Missing Authentication for Critical Function**

**Vulnerabilities**

| CVE ID | Base Severity | Description |
|---|---|---|
| **CVE-2025-13777** | High | An unauthenticated query reveals data. Authentication Bypass due to Improper Session Validation. |
| **CVE-2025-13778** | Medium | An unauthenticated query allows an attacker to remotely reboot the device, potentially causing a denial of service. |
| **CVE-2025-13779** | High | An unauthenticated query reveals the system configuration, including sensitive details. |

**Remediations:**
The following product versions have been fixed:

- ABB AWIN Firmware 2.1-0 installed on ABB AWIN GW100 rev. 2 (Product ID: 3BNP102988R1) are fixed versions for CVE-2025-13777, CVE-2025-13778 and CVE-2025-13779.
- ABB AWIN Firmware2.0-0 installed on ABB AWIN GW120 (Product ID 3BNP103003R1) are fixed versions for CVE-2025-13777, CVE-2025-13778 and CVE-2025-13779.

## ABB Ability Symphony Plus Engineering

**Summary**

ABB became aware of vulnerability in the products versions listed as affected in the advisory. The ABB S+ Engineering product versions are affected by vulnerabilities in PostgreSQL version 13.11 and earlier versions. If an attacker gains access to a site's S+ Client Server network, they could exploit such vulnerabilities by executing arbitrary code and potentially compromising the entire system.

The following versions of Siemens SCALANCE are affected:

- **Ability Symphony Plus 2.2, 2.3, 2.3_RU1, 2.3_RU2, 2.3_RU3, 2.4, 2.4_SP1, 2.4_SP2, 2.4_SP2_RU1**

- **CVSS v3 8.8**
- **Vendor: ABB**
- **Equipment: ABB Ability Symphony Plus Engineering**
- **Vulnerabilities: Integer Overflow or Wraparound, Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection'), Time-of-check Time-of-use (TOCTOU) Race Condition, Privilege Dropping / Lowering Errors**

**Vulnerabilities**

| CVE ID | Base Severity | Description |
|---|---|---|
| **CVE-2023-5869** | High | An attacker running as an authenticated PostgreSQL user can provide crafted data and trigger the integer overflow due to such missing overflow check. This can enable the execution of arbitrary code in the system. |
| **CVE-2023-39417** | High | If an administrator has installed Extension scripts and specific data is used inside a quoting con-struct, an attacker having proper PostgreSQL privileges can execute arbitrary code in the system as |

| | | |
|---|---|---|
| | | the administrator. |
| **CVE-2024-7348** | High | A 'time-of-check time-of-use' (TOCTOU) race condition in a PostgreSQL can allow an attacker to easily execute arbitrary SQL functions by leveraging a PostgreSQL utility often executed with high privileges. |
| **CVE-2024-0985** | High | An attacker can provide untrusted materialized views and lure a high privileged authorized user to inadvertently execute arbitrary SQL functions by refreshing the attacker's materialized view. |

**Remediations:**
ABB advises all customers to review their installations to determine if they are using an impacted product as listed above, no further analysis or tools are needed to make this determination. The recommended immediate actions per product are listed below: - Systems using S+ Engineering 2.2 through 2.4 SP2 should upgrade to S+ Engineering 2.4 SP2 RU1 (re-leased in December 2024) or later. - End users who are unable to install one of these updates should immediately look to implement the Mitigation and Workarounds listed below as this will restrict or prevent an attacker's ability to compromise the system. ABB recommends that customers apply the update at the earliest convenience.

**Mitigation:**
Any exploit of these vulnerabilities would require that the attacker has access to the site's S+ client/server network. Following ABB's recommended security practices, including network architecture and perimeter firewall, are mitigating factors in preventing external access to the S+ client/server network. Refer to section "General security recommendations" for further advise on how to keep your system secure.

## References

https://www.cisa.gov/news-events/ics-advisories/icsa-26-120-01
https://www.cisa.gov/news-events/ics-advisories/icsa-26-120-02
https://www.cisa.gov/news-events/ics-advisories/icsa-26-120-03
https://www.cisa.gov/news-events/ics-advisories/icsa-26-120-04
https://www.cisa.gov/news-events/ics-advisories/icsa-26-120-05
https://www.cisa.gov/news-events/ics-advisories/icsa-26-120-06

## CVEs

CVE-2025-3756
CVE-2018-1002208
CVE-2025-10571
CVE-2025-14510
CVE-2025-13777
CVE-2025-13778
CVE-2025-13779
CVE-2023-5869
CVE-2023-39417
CVE-2024-7348
CVE-2024-0985

Smarttech
YOUR 24/7 SECURITY PARTNER

www.smarttech247.com