

|   |                           |                           |   |
|---|---------------------------|---------------------------|---|
| Document ID<br><b>AAES-Insight-2023-001</b> | Revision<br><b>1</b>      | Date<br><b>2023-11-03</b> | Document category<br><b>Product Security Advisory</b> |
| Confidentiality level<br><b>Public</b>      | Status<br><b>Approved</b> |                           | Page (of)<br><b>1 (2)</b>                             |

**TLP:WHITE**

Disclosure is not limited.

# AAES-Insight-2023-001: Insight Login Page vulnerable to Clickjacking

## Date

2023-11-03

## Overview

A clickjacking vulnerability has been discovered on the Insight web application login page. This vulnerability could allow an attacker to embed a malicious website on top of the Insight Login page using an iframe, which tricks users into performing unintended actions.

Our investigation followed our vulnerability handling process covering investigation, remediation, post-remediation, and security advisory publication.

## Affected Products

The clickjacking vulnerability affects only the Insight web application Login Page.

## Description

An attacker can exploit this vulnerability by creating a page that includes a hidden iframe with the Insight Login Page and overlay this invisible frame on top of a page it controls. This could trick users into performing unintended actions when they visit the page.

## Impact

Successful exploitation of this vulnerability could trick users into performing unintended actions, such as disclosing their passwords, personal information, or malware distribution.

## Severity

6.5 Medium – CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N.

## Remediation

|   |                           |                           |   |
|---|---------------------------|---------------------------|---|
| Document ID<br><b>AAES-Insight-2023-001</b> | Revision<br><b>1</b>      | Date<br><b>2023-11-03</b> | Document category<br><b>Product Security Advisory</b> |
| Confidentiality level<br><b>Public</b>      | Status<br><b>Approved</b> |                           | Page (of)<br><b>2 (2)</b>                             |

We have enhanced our security by implementing a new response header policy to restrict clickjacking. This policy effectively mitigates the risk of unauthorized embedding of our content within other websites.

## References

- <https://nvd.nist.gov/vuln/detail/CVE-2017-5697>
- <https://cwe.mitre.org/data/definitions/1021.html>

## Credit

This vulnerability was discovered and researched by **Vaibhav Shinde**.

## Contact Information

For further inquiries, questions, or clarifications on vulnerabilities, contact us via [aaesproduct.security@assaabloy.com](mailto:aaesproduct.security@assaabloy.com).

## Revision History

| Revision | Date       | Description         |
|----------|------------|---------------------|
| 1        | 2023-11-22 | Initial Publication |

## 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 TO THIS DOCUMENT IS AT YOUR OWN RISK. ASSA ABLOY ENTRANCE SYSTEMS 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 ENTRANCE SYSTEMS PRODUCTS.