# SSA-580228: Use of Hard-Coded Credentials Vulnerability in Location Intelligence before V4.3

Publication Date: 2024-02-13
Last Update: 2024-02-13
Current Version: V1.0
CVSS v3.1 Base Score: 9.8
CVSS v4.0 Base Score: 9.3

## SUMMARY

Location Intelligence before V4.3 is affected by a Use of Hard-coded Credentials vulnerability that could allow an attacker to obtain full administrative access to the application.

Siemens has released new versions for the affected products and recommends to update to the latest versions.

## AFFECTED PRODUCTS AND SOLUTION

| Affected Product and Versions | Remediation |
|---|---|
| Location Intelligence Perpetual Large (9DE5110-8CA13-1AX0):<br>All versions < V4.3<br>affected by all CVEs | Update to V4.3 or later version. The update is available from Siemens Online Software Delivery (OSD). |
| Location Intelligence Perpetual Medium (9DE5110-8CA12-1AX0):<br>All versions < V4.3<br>affected by all CVEs | Update to V4.3 or later version. The update is available from Siemens Online Software Delivery (OSD). |
| Location Intelligence Perpetual Non-Prod (9DE5110-8CA10-1AX0):<br>All versions < V4.3<br>affected by all CVEs | Update to V4.3 or later version. The update is available from Siemens Online Software Delivery (OSD). |
| Location Intelligence Perpetual Small (9DE5110-8CA11-1AX0):<br>All versions < V4.3<br>affected by all CVEs | Update to V4.3 or later version. The update is available from Siemens Online Software Delivery (OSD). |
| Location Intelligence SUS Large (9DE5110-8CA13-1BX0):<br>All versions < V4.3<br>affected by all CVEs | Update to V4.3 or later version. The update is available from Siemens Online Software Delivery (OSD). |
| Location Intelligence SUS Medium (9DE5110-8CA12-1BX0):<br>All versions < V4.3<br>affected by all CVEs | Update to V4.3 or later version. The update is available from Siemens Online Software Delivery (OSD). |
| Location Intelligence SUS Non-Prod (9DE5110-8CA10-1BX0):<br>All versions < V4.3<br>affected by all CVEs | Update to V4.3 or later version. The update is available from Siemens Online Software Delivery (OSD). |

| | |
|---|---|
| Location Intelligence SUS Small (9DE5110-8CA11-1BX0):<br>All versions < V4.3<br>affected by all CVEs | Update to V4.3 or later version. The update is available from Siemens Online Software Delivery (OSD). |

## WORKAROUNDS AND MITIGATIONS

Product-specific remediations or mitigations can be found in the section Affected Products and Solution. Please follow the General Security Recommendations.

## GENERAL SECURITY RECOMMENDATIONS

As a general security measure, Siemens strongly recommends to protect network access to devices with appropriate mechanisms. In order to operate the devices in a protected IT environment, Siemens recommends to configure the environment according to Siemens' operational guidelines for Industrial Security (Download: https://www.siemens.com/cert/operational-guidelines-industrial-security), and to follow the recommendations in the product manuals. Additional information on Industrial Security by Siemens can be found at: https://www.siemens.com/industrialsecurity

## PRODUCT DESCRIPTION

Location Intelligence is a web-based application software that, based on position data, creates transparency in production and logistics processes and thus uncovers potential for optimization.

Location Intelligence Software Update Service (SUS) contains all available software update for 1 year (conditions: see SUS certificate).

## VULNERABILITY DESCRIPTION

This chapter describes all vulnerabilities (CVE-IDs) addressed in this security advisory. Wherever applicable, it also documents the product-specific impact of the individual vulnerabilities.

### Vulnerability CVE-2024-23816

Affected products use a hard-coded secret value for the computation of a Keyed-Hash Message Authentication Code. This could allow an unauthenticated remote attacker to gain full administrative access to the application.

| | |
|---|---|
| CVSS v3.1 Base Score | 9.8 |
| CVSS Vector | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C |
| CVSS v4.0 Base Score | 9.3 |
| CVSS Vector | CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N |
| CWE | CWE-798: Use of Hard-coded Credentials |

## ADDITIONAL INFORMATION

For further inquiries on security vulnerabilities in Siemens products and solutions, please contact the Siemens ProductCERT:

https://www.siemens.com/cert/advisories

## HISTORY DATA

V1.0 (2024-02-13): Publication Date

## TERMS OF USE