# SSA-480824: Multiple Vulnerabilities in LOGO! 8 BM

Publication Date: 2020-12-08
Last Update: 2020-12-08
Current Version: V1.0
CVSS v3.1 Base Score: 9.8

## SUMMARY

The latest update for LOGO! 8 BM fixes multiple vulnerabilities. The most severe could allow an attacker with network access to gain full control over the device.

Siemens has released updates for the affected products and recommends that customers update to the latest version.

## AFFECTED PRODUCTS AND SOLUTION

| Affected Product and Versions | Remediation |
|---|---|
| LOGO! 8 BM (incl. SIPLUS variants):<br>All versions < V8.3 | Update to V8.3. Notice that in order to update, a new hardware version is required.<br>https://support.industry.siemens.com/cs/ww/en/view/109783346/ |
| LOGO! Soft Comfort:<br>All versions < V8.3<br>only affected by CVE-2020-25231, CVE-2020-25234 | Update to V8.3<br>https://support.industry.siemens.com/cs/ww/en/view/109783154/ |

## WORKAROUNDS AND MITIGATIONS

Siemens has identified the following specific workarounds and mitigations that customers can apply to reduce the risk:

- Apply Defense-in-Depth concept, including protection concept outlined in the system manual.

## 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

Siemens LOGO! BM (Base Module) devices are used for basic small-scale automation tasks.

LOGO! Soft Comfort is an engineering software to configure and program LOGO! BM (Base Module) devices

SIPLUS extreme products are designed for reliable operation under extreme conditions and are based on SIMATIC, LOGO!, SITOP, SINAMICS, SIMOTION, SCALANCE or other devices. SIPLUS devices use the

same firmware as the product they are based on.

## VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.1 (CVSS v3.1) (https://www.first.org/cvss/). The CVSS environmental score is specific to the customer's environment and will impact the overall CVSS score. The environmental score should therefore be individually defined by the customer to accomplish final scoring.

An additional classification has been performed using the CWE classification, a community-developed list of common software security weaknesses. This serves as a common language and as a baseline for weakness identification, mitigation, and prevention efforts. A detailed list of CWE classes can be found at: https://cwe.mitre.org/.

### Vulnerability CVE-2020-25228

A service available on port 10005/tcp of the affected devices could allow complete access to all services without authorization. An attacker could gain full control over an affected device, if he has access to this service. The system manual recommends to protect access to this port.

| | |
|---|---|
| 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 |
| CWE | CWE-306: Missing Authentication for Critical Function |

### Vulnerability CVE-2020-25229

The implemented encryption for communication with affected devices is prone to replay attacks due to the usage of a static key. An attacker could change the password or change the configuration on any affected device if using prepared messages that were generated for another device.

| | |
|---|---|
| CVSS v3.1 Base Score | 8.1 |
| CVSS Vector | CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C |
| CWE | CWE-321: Use of Hard-coded Cryptographic Key |

### Vulnerability CVE-2020-25230

Due to the usage of an outdated cipher mode on port 10005/tcp, an attacker could extract the encryption key from a captured communication with the device.

| | |
|---|---|
| CVSS v3.1 Base Score | 5.9 |
| CVSS Vector | CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C |
| CWE | CWE-327: Use of a Broken or Risky Cryptographic Algorithm |

### Vulnerability CVE-2020-25231

The encryption of program data for the affected devices uses a static key. An attacker could use this key to extract confidential information from protected program files.

| | |
|---|---|
| CVSS v3.1 Base Score | 6.2 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C |
| CWE | CWE-321: Use of Hard-coded Cryptographic Key |

Vulnerability CVE-2020-25232

Due to the usage of an insecure random number generation function and a deprecated cryptographic function, an attacker could extract the key that is used when communicating with an affected device on port 8080/tcp.

| | |
|---|---|
| CVSS v3.1 Base Score | 5.9 |
| CVSS Vector | CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C |
| CWE | CWE-327: Use of a Broken or Risky Cryptographic Algorithm |

Vulnerability CVE-2020-25233

The firmware update of affected devices contains the private RSA key that is used as a basis for encryption of communication with the device.

| | |
|---|---|
| CVSS v3.1 Base Score | 6.2 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C |
| CWE | CWE-321: Use of Hard-coded Cryptographic Key |

Vulnerability CVE-2020-25234

The LOGO! program files generated and used by the affected components offer the possibility to save user-defined functions (UDF) in a password protected way. This protection is implemented in the software that displays the information. An attacker could reverse engineer the UDFs directly from stored program files.

| | |
|---|---|
| CVSS v3.1 Base Score | 7.7 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C |
| CWE | CWE-321: Use of Hard-coded Cryptographic Key |

Vulnerability CVE-2020-25235

The password used for authentication for the LOGO! Website and the LOGO! Access Tool is sent in a recoverable format. An attacker with access to the network traffic could derive valid logins.

| | |
|---|---|
| CVSS v3.1 Base Score | 5.9 |
| CVSS Vector | CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C |
| CWE | CWE-522: Insufficiently Protected Credentials |

## ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Tobias Gebhardt for coordinated disclosure of CVE-2020-25228
- Thomas Meesters from cirosec GmbH for coordinated disclosure of CVE-2020-25229 to CVE-2020-25234
- Max Bäumler for coordinated disclosure of CVE-2020-25235

## 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 (2020-12-08): Publication Date

## TERMS OF USE