# SSA-709003: Privilege Escalation Vulnerability in License Management Utility (LMU)

| | |
|---|---|
| Publication Date: | 2020-09-08 |
| Last Update: | 2020-09-08 |
| Current Version: | V1.0 |
| CVSS v3.1 Base Score: | 7.8 |

## SUMMARY

The latest update for the License Management Utility (LMU), which is used by multiple Siemens building technology products, fixes a vulnerability that could allow local users to escalate privileges and execute code as local SYSTEM user.

Siemens has released an update version of LMU, recommends to install this update on all affected systems and provides specific countermeasures for yet unpatched systems.

## AFFECTED PRODUCTS AND SOLUTION

| Affected Product and Versions | Remediation |
|---|---|
| License Management Utility (LMU):<br>All versions < V2.4 | Update to V2.4<br>https://support.industry.siemens.com/cs/document/109479834 |

## WORKAROUNDS AND MITIGATIONS

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

- Apply security hardening of the Windows Server, where LMU is installed on, in accordance with your corporate security policies or up-to-date hardening guidelines
- Ensure that only trusted persons have access to the system and avoid the configuration of additional local accounts on the server

## GENERAL SECURITY RECOMMENDATIONS

As a general security measure Siemens strongly recommends to protect network access to affected products with appropriate mechanisms. It is advised to follow recommended security practices in order to run the devices in a protected IT environment.

## PRODUCT DESCRIPTION

License Management Utiliy (LMU) is the unified license management system for Siemens' building automation products such as Desigo CC and ABT.

## 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-2020-10056

The lmgrd service of the affected application is executed with local SYSTEM privileges on the server while its configuration can be modified by local users.

The vulnerability could allow a local authenticated attacker to execute arbitrary commands on the server with local SYSTEM privileges.

| | |
|---|---|
| CVSS v3.1 Base Score | 7.8 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C |
| CWE | CWE-250: Execution with Unnecessary Privileges |

## ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Bundesamt für Sicherheit in der Informationstechnik (BSI) for reporting the vulnerability

## 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 (2020-09-08): | Publication Date |

## TERMS OF USE

Siemens Security Advisories are subject to the terms and conditions contained in Siemens' underlying license terms or other applicable agreements previously agreed to with Siemens (hereinafter "License Terms"). To the extent applicable to information, software or documentation made available in or through a Siemens Security Advisory, the Terms of Use of Siemens' Global Website (https://www.siemens.com/terms_of_use, hereinafter "Terms of Use"), in particular Sections 8-10 of the Terms of Use, shall apply additionally. In case of conflicts, the License Terms shall prevail over the Terms of Use.