SSA-151221: Incorrect File Permissions in APOGEE Insight

Publication Date 2016-03-18
Last Update 2017-02-13
Current Version V1.1
CVSSv3 Base Score 3.4

SUMMARY

APOGEE Insight is affected by a vulnerability that could allow authenticated operating system users to modify application data under certain conditions.

Siemens has released a new APOGEE Insight version which resolves the vulnerability.

AFFECTED PRODUCTS

APOGEE Insight: All versions < V3.15

DESCRIPTION

APOGEE Insight software provides an easy-to-use graphical interface to manage and control a building.

Detailed information about the vulnerability is provided below.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3 (CVSSv3) (http://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.

Vulnerability Description (CVE-2016-3155)

The file permissions set for the APOGEE Insight application folder could allow authenticated operating system users for the modification of APOGEE Insight application data if local access was obtained.

Base Score 3.4
Vector CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C

Mitigating Factors

The attacker must have local access to the filesystem.

SOLUTION

Siemens provides APOGEE Insight V3.15 [1], which fixes the vulnerability.

ACKNOWLEDGEMENTS

Siemens thanks the following for their support and efforts:

- China Electronic Technology Cyber Security Co., Ltd. for coordinated disclosure of the vulnerability.
- Hunan Testing Institute of Product and Commodity Supervision for coordinated disclosure of the vulnerability.

ADDITIONAL RESOURCES

[1] Please call your local service organization for further information on how to obtain and apply V3.15. If assistance in identifying your local service organization is required, please call a local Siemens hotline center:
https://w3.siemens.com/aspa_app/

[2] For further inquiries on vulnerabilities in Siemens products and solutions, please contact the Siemens ProductCERT:
https://www.siemens.com/cert/advisories

HISTORY DATA

V1.0 (2016-03-18): Publication Date
V1.1 (2017-02-13): Added patch information for APOGEE Insight

DISCLAIMER