GE Industrial Solutions Product Security Advisory

Title:	UPS SNMP Adapter Command Injection and Storage of Sensitive Information Vulnerabilities
Vulnerability ID:	GEIS16-01
Other identifiers:	CVE-2016-0861, CVE-2016-0862
Release date:	January 27, 2016
Last updated:	January 25, 2016
Revision:	2

Summary

Two vulnerabilities have been identified in the SNMP/Web Interface adapter for Uninterruptible Power Supplies that, if exploited, could allow an adversary to execute arbitrary system commands and gain access to sensitive user's account information.

GE Industrial Solutions recommends that customers install the latest SNMP/Web Interface adapter with firmware version 4.8, which has been updated to address the vulnerabilities.

Affected Products

- All SNMP/Web Interface cards with firmware version prior to 4.8 manufactured by GE Industrial Solutions.

Solutions

Installing firmware version 4.8 on the SNMP/Web Interface adapters with the following P/N will address these issues. In particular:

- 1024746
- 1024747
- 1024748
- 1024921

All other P/Ns will need to be upgraded to the latest hardware version of the product with firmware 4.8.

To obtain additional information on solution options, affected customers can contact connectivity-ups@ge.com

Vulnerability information

Due to lack of proper input validation, an authenticated user can execute arbitrary system commands that could potentially impact confidentiality, integrity, and availability of the SNMP/Web Interface adapter.

Exploitation of the cleartext storage of sensitive information may allow an authenticated user with lesser privilege to access other users' sensitive account information, leading to gaining access to the adapter at higher privilege level.

Acknowledgements

GE Industrial Solutions would like to thank Karn Ganeshen for reporting this issue via ICS-CERT and for helping to protect our customers.

Disclaimer

Change Log

Revision	Date	Change(s)
1	January 20, 2016	• Initial release
2	January 25, 2016	• Updated CVE references