

Subject 2900-2-2

May 11, 2018

SUMMARY OF TOPICS

The following topics for the Standard for Software Cybersecurity for Network-Connectable Products, Part 2-2: Particular Requirements for Industrial Control Systems, UL 2900-2-2, are being recirculated:

1. Proposed first edition of the Standard for Software Cybersecurity for Network-Connectable Products, Part 2-2: Particular Requirements for Industrial Control Systems, UL 2900-2-2

COMMENTS DUE: JUNE 11, 2018

For your convenience in review, proposed additions to the previously proposed requirements dated 2017-09-15 are shown underlined and proposed deletions are shown ~~lined-out~~.

1. Proposed first edition of the Standard for Software Cybersecurity for Network-Connectable Products, Part 2-2: Particular Requirements for Industrial Control Systems, UL 2900-2-2

RATIONALE

Responses to comments have been posted within the UL 2900-2-2 Proposal Review Work Area dated 2017-09-15.

PROPOSAL

8.6 An attempt to randomly provide a credential shall have ~~at a minimum~~less than a one in 1,000,000 success rate.

~~8.7 The information by itself cannot be used for authentication but is input in a split knowledge procedure. Documentation shall prove that only access of ALL components in the split knowledge has the ability to determine the information.~~

~~8.8 The transmission path is a trusted path, for example a directly connected physical cable that is not shared by any other system or products.~~

8.8.1 The transmission of the authentication credential to a product via a remote connection covered in this section cannot be in plain text or easily intercepted and duplicated unless:

a) Parts of the credential itself cannot be used for authentication but is input in a split knowledge procedure. Documentation shall prove that only access of ALL components in the split knowledge has the ability to determine the information.

b) The transmission path is a trusted path, for example a directly connected physical cable that is not shared by any other system or products.

**UL COPYRIGHTED MATERIAL –
NOT AUTHORIZED FOR FURTHER REPRODUCTION OR
DISTRIBUTION WITHOUT PERMISSION FROM UL**



Documents
Document Sharing Hub

8.9 The storage of the authentication credential(s) on the product shall not be in plaintext and shall be protected from unauthorized disclosure or modification by using one of the cryptography mechanisms defined in Section 10, Sensitive Data.

11.2 The product shall be able to reliably and verifiably display or communicate the version of the currently installed software and firmware binaries, executables and libraries to the user of the product that identifies the version of the software for the product.

11.3 The software deployment process shall follow:

- a) The new software and firmware binaries, executables and libraries shall be created with a software integrity mechanism to generate a factory code or signature for the binary. These mechanisms shall meet Appendix C of the Standard for Software Cybersecurity for Network-Connectable Devices, Part 1: General Requirements, UL 2900-1.
- b) Deployment of the software/firmware binaries, executables and libraries to the product shall begin with the download of the software/firmware binaries, executables, and libraries. ~~It shall not alter the product~~The download shall not immediately update the stored executables during the download process unless specified in the risk assessment.
- ~~dc)~~ The product may allow the erasure of the audit log via operator intervention to allow for download of the software/firmware binaries, executables, and libraries only if, at a minimum, the product ~~should start~~starts the new log with a record of the log erasure including the timestamp, and authenticated means and account.

11.4 After the download of the software/firmware binaries, executables and libraries and before the ~~installation of it~~installing them, the product shall verify the integrity and the authenticity of the software /firmware binaries, executables and libraries.

- a) If the integrity test fails, the product shall stop the software upgrade process, and shall erase the new downloaded software component. A failure shall be logged in the audit log. The product shall continue to operate as intendedbefore the attempted upgrade.
- b) The product shall carry out the integrity check only when the product has received the complete software, consisting of the software/firmware binaries, executables, and libraries.
- c) The integrity mechanism shall be included in the software/firmware binaries, executables, and libraries and shall not be downloaded separately.

11.7 If the product fails section 11.6 on any power up, the product shall enter a FAIL safe mode and indicate clearly to the user that the product has failed to start up successfully.

15.2.2 Discrete Output Behavior - While the conditions of Section 15.1.1 are met, the product shall be able to generate a monitored continuous output signal ~~while the conditions of Section 15.1.1 are met~~ on one of the output points in a discrete output module as specified by the manufacturer specifications.

Copyright © 2018 Underwriters Laboratories Inc.