

SA-SYS-2019-001: Undocumented service access

Publication Date: 2019-04-12
Last Update: 2019-04-12
Version: V1.0
Severity: Critical

CVE Identifier

CVE-2019-10712

Description

The reported vulnerability allows a remote attacker to change the settings or exchange the application of the device.

Impact

By exploiting the undocumented service access, it is possible to change the settings of a device. The service access user has access to the web based management with administrator privileges. This can be potentially used to lock other users out from the device or to open closed network ports. It is also possible to use this service access as FTP user and exchange or delete the application.

Affected Products

The following products with a firmware prior to FW14 are affected by this vulnerability:

- Series 750-88x
 - 750-330 (<FW14)
 - 750-352/... (<FW14)
 - 750-829 (<FW14)
 - 750-831/... (<FW14)
 - 750-852 (<FW14)
 - 750-880/... (<FW14)
 - 750-881 (<FW14)
 - 750-882 (<FW14)
 - 750-884/... (<FW14)
 - 750-885/... (<FW14)
 - 750-889 (<FW14)

- Series 750-87x
 - 750-830 (<FW06)
 - 750-849 (<FW08)
 - 750-871 (<FW11)
 - 750-872 (<FW07)
 - 750-873 (<FW07)

Vulnerability Characterization

Use of Hard-coded Credentials (CWE-798)

CVSS Base Score: 9.8
Impact Subscore: 5.9
Exploitability Subscore: 3.9

Overall CVSS Score: 9.8

The service access allows a remote attacker to change the device settings by using the web-based management or exchange / delete the application after open the ftp port.

Solution

Update your device to the latest firmware:

750-330	(>= FW 14)
750-352/...	(>= FW 14)
750-829	(>= FW 14)
750-831/...	(>= FW 14)
750-852	(>= FW 14)
750-880/...	(>= FW 14)
750-881	(>= FW 14)
750-882	(>= FW 14)
750-884/...	(>= FW 14)
750-885/...	(>= FW 14)
750-889	(>= FW 14)
750-871	(>= FW 11)
750-872	(>= FW 07)
750-873	(>= FW 07)
750-849	(>= FW 08)
750-830	(>= FW 06)

Mitigation

- Restrict network access to the web server.
- Restrict network access to the device.
- Do not directly connect the device to the internet.

Additional Resources

None

Reported

Reported by Jörn Schneeweisz / Reurity Labs to CERT-Bund coordinated by CERT@VDE.

Disclaimer

The security instructions given here have exclusively technical-informatory character; contractual stipulations remain unaffected.



<http://global.wago.com/en/wago/impressum/software-user-agreement/index.jsp>

For updates please visit <https://cert.vde.com/de-de> regularly, in case of any questions please contact your local sales representative or send your question by email to security@wago.com.