SA-SYS-2019-002: Hardcoded Users And Passwords

Publication Date: 2019-06-05
Last Update: 2019-06-05
Version: V1.0
Severity: Critical

CVE Identifier

CVE-2019-12550

Description

The reported vulnerability allows a remote attacker to change the settings of the managed switch.

Impact

By exploiting the hardcoded credentials, it is possible to change the settings of the managed switch. The hardcoded user has access to the CLI with root privileges. This can be potentially used to manipulate the switch settings.

Affected Products

The following products with a firmware prior to the one that is listed are affected by this vulnerability:

- Series 852
  - 852-303 (<V1.2.2.S0)
  - 852-1305 (<V1.1.6.S0)
  - 852-1505 (<V1.1.5.S0)

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 switch settings by using the CLI interface or log into the operating system.
Solution

Update your managed switch to the latest firmware:

- 852-303 (>= V1.2.2.S0)
- 852-1305 (>= V1.1.6.S0)
- 852-1505 (>= V1.1.5.S0)

Mitigation

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

Additional Resources

None

Reported

Reported by T. Weber / SEC Consult Vulnerability Lab to CERT@VDE.

Disclaimer

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


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.