SA-SYS-2019-003: Hardcoded Private Keys For The SSH Daemon

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

CVE Identifier

CVE-2019-12549

Description

The reported vulnerability allows a remote attacker to compromise the managed switch.

Impact

By exploiting the hardcoded SSK key, it is possible to disrupt communication or compromise the managed switch. Because these SSH-keys cannot be regenerated by users, all switches use the same key.

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 Cryptographic Key (CWE-321)

CVSS Base Score: 10.0  
Impact Subscore: 6.0  
Exploitability Subscore: 3.9  

Overall CVSS Score: 10.0

A hard-coded cryptographic key vulnerability was identified. Vulnerable versions of the managed switches use hard-coded SSH keys.
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.