VULNERABLE FIRMWARE VERIFICATION

Date	5 December 2022, Version 1.0
Sensitivity	**TLP:GREEN**
Relevance	SPRECON-E-C/-E-P/-E-T3: ***affected*** SPRECON-V460: ***not affected***
Description	A vulnerable firmware verification in the firmware of the SPRECON-E product range has been identified. Through physical access and hardware manipulation, an attacker might be able to bypass hardware-based code verification and thus inject arbitrary code. **Affected Product**: SPRECON-E-C/P/T3 CPU modules of following variants: PU244x **Solution** Sprecher Automation will address this vulnerability by providing firmware updates together with improved boot loaders. We will inform once new firmware is available. **Mitigation** The access vector is bound to physical device access. Hence, it is recommended to emphasize physical security controls. See general recommendations. Besides this, it needs to be taken into account that necessary hardware manipulation to fully exploit this vulnerability requires to put the device out of operation for several time; i.e. device status monitoring as usually applied in substation automation is an important measure to also detect potential attacks. **General Recommendations** Sprecher Automation strongly recommends to emphasize security best practices in critical infrastructures such as e.g. measures according to ISO/IEC 27019. Hence, both network as well as physical access to OT devices need to be restricted to a minimum, while protecting and monitoring all access means. Also, engineering / remote maintenance infrastructure needs to be protected with high security in mind, as potentially sensitive configuration data or maintenance access credentials could be stored there.

SEVERITY EVALUATION

Evaluation	**Common Vulnerability Scoring System (CVSS)**
CVSS v3	**Base Score:** 6.8 **Temporal Score:** 6.6 **Environmental Score:** 6.6 **Vector:** CVSS:3.0/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:F/RL:U/RC:C/CR:H/IR:H/AR:H/MAV:P/MAC:L/MPR:N/MUI:N/MS:U/MC:H/MI:H/MA:H

HARDENING NOTIFICATION: SPRECON MAINTENANCE ACCESS WITH HARDCODED CREDENTIALS

Date	5 December 2022, Version 1.0
Sensitivity	**TLP:GREEN**
Relevance	SPRECON-E-C/-E-P/-E-T3: ***affected*** SPRECON-V460: ***not affected***
Description	SPRECON-E devices offer the ability to enable maintenance logins; these maintenance logins use static credentials that are only known to limited Sprecher staff but shall only be enabled by the device owner in case of explicit necessity. According to Sprecher's hardening guidelines, these accounts shall be disabled for operation. Disabling can be done via normal configuration access which in turn shall be secured with SPRECON's RBAC (role-based access control). This information is meant to again put attention to this hardening measure. It is recommended to check if maintenance access is disabled. Additionally, access to devices' configuration files that are stored on engineering PC systems shall be limited and monitored. Overall, SPRECON hardening guidelines are always recommended to be implemented in case this has not been done so far. In a coming firmware release, device owners will additionally have the ability to gain more control over these user accounts by not only being able to disable them, but also by setting individual credentials in case their usage is necessary. The maintenance user accounts are equipped with limited privileges and e.g. do not have access to stored keys in the device. **Affected Product**: SPRECON-E CPU modules of following variants: - PU243x, PU244x - MC33/34 - SPRECON-EDIR **General Recommendations** Sprecher Automation strongly recommends to emphasize security best practices in critical infrastructures such as e.g. measures according to ISO/IEC 27019. Hence, both network as well as physical access to OT devices need to be restricted to a minimum, while protecting and monitoring all access means. Also, engineering / remote maintenance infrastructure needs to be protected with high security in mind, as potentially sensitive configuration data or maintenance access credentials could be stored there.

SEVERITY EVALUATION

Evaluation	**Common Vulnerability Scoring System (CVSS)**
CVSS v3	**Base Score:** 6.7

	Temporal Score: 6.5 **Environmental Score:** 7.0 **Vector:** CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:H/A:H/E:H/RL:W/RC:C/CR:H/IR:H/AR:H/MAV:N/MAC:L/MPR:H/MUI:N/MS:U/MC:L/MI:H/MA:H