# CVE Detail – CVE-2022-30320

Saia Burgess Controls (SBC) PCD through 2022-05-06 uses a Broken or Risky Cryptographic Algorithm. According to FSCT-2022-0063, there is a Saia Burgess Controls (SBC) PCD S-Bus weak credential hashing scheme issue. The affected components are characterized as: S-Bus (5050/UDP) authentication. The potential impact is: Authentication bypass. The Saia Burgess Controls (SBC) PCD controllers utilize the S-Bus protocol (5050/UDP) for a variety of engineering purposes. It is possible to configure a password in order to restrict access to sensitive engineering functionality. Authentication is done by using the S-Bus 'write byte' message to a specific address and supplying a hashed version of the password. The hashing algorithm used is based on CRC-16 and as such not cryptographically secure. An insecure hashing algorithm is used. An attacker capable of passively observing traffic can intercept the hashed credentials and trivially find collisions allowing for authentication without having to bruteforce a keyspace defined by the actual strength of the password. This allows the attacker access to sensitive engineering functionality such as uploading/downloading control logic and manipulating controller configuration.

## Threat-Mapped Scoring

Score: 3.25

Priority: P2 - Serious (High)

## EPSS

EPSS Score: N/A

Percentile: 0.00125

## CVSS Scoring

CVSS v3.1 Score: 4.3

Severity: MEDIUM

## Mapped CWE(s)

* CWE-327: Use of a Broken or Risky Cryptographic Algorithm

## CAPEC(s)

* CAPEC-20: Encryption Brute Forcing
* CAPEC-459: Creating a Rogue Certification Authority Certificate
* CAPEC-473: Signature Spoof
* CAPEC-475: Signature Spoofing by Improper Validation
* CAPEC-608: Cryptanalysis of Cellular Encryption
* CAPEC-614: Rooting SIM Cards
* CAPEC-97: Cryptanalysis

## ATT&CK Techniques

* T1553.002: Code Signing
* T1036.001: Invalid Code Signature

## Used By (Actors/Tools)

* TrickBot (malware)
* BLINDINGCAN (malware)
* Stuxnet (malware)
* WindTail (malware)
* StrongPity (malware)
* Janicab (malware)
* Ecipekac (malware)
* NETWIRE (malware)
* GreyEnergy (malware)
* Regin (malware)
* CHIMNEYSWEEP (malware)
* BOOSTWRITE (malware)
* SpicyOmelette (malware)
* LockerGoga (malware)
* Anchor (malware)
* Lumma Stealer (malware)
* Epic (malware)
* Gazer (malware)
* Metamorfo (malware)
* Bandook (malware)
* PipeMon (malware)
* Black Basta (malware)
* ZeroCleare (malware)
* RTM (malware)
* StrelaStealer (malware)
* GoBear (malware)
* Bazar (malware)
* HermeticWiper (malware)
* Cobalt Strike (malware)
* SUNBURST (malware)
* Daserf (malware)
* MacMa (malware)
* ROADSWEEP (malware)
* More\_eggs (malware)
* SysUpdate (malware)
* BackConfig (malware)
* Nerex (malware)
* Clop (malware)
* Troll Stealer (malware)
* Ebury (malware)
* ChChes (malware)
* AppleJeus (malware)
* BADNEWS (malware)
* QakBot (malware)
* Gelsemium (malware)
* Helminth (malware)
* HermeticWizard (malware)
* PcShare (tool)
* CSPY Downloader (tool)
* QuasarRAT (tool)
* LuminousMoth (intrusion-set)
* Wizard Spider (intrusion-set)
* FIN7 (intrusion-set)
* APT41 DUST (campaign)
* OilRig (intrusion-set)
* SolarWinds Compromise (campaign)
* Lazarus Group (intrusion-set)
* Daggerfly (intrusion-set)
* TA505 (intrusion-set)
* Suckfly (intrusion-set)
* FIN6 (intrusion-set)
* Silence (intrusion-set)
* Patchwork (intrusion-set)
* Darkhotel (intrusion-set)
* Operation Honeybee (campaign)
* Kimsuky (intrusion-set)
* Leviathan (intrusion-set)
* RedDelta Modified PlugX Infection Chain Operations (campaign)
* menuPass (intrusion-set)
* Moses Staff (intrusion-set)
* Operation Dream Job (campaign)
* Molerats (intrusion-set)
* APT37 (intrusion-set)
* APT41 (intrusion-set)
* GALLIUM (intrusion-set)
* C0015 (campaign)
* Winnti Group (intrusion-set)
* Saint Bear (intrusion-set)
* Scattered Spider (intrusion-set)
* Windshift (intrusion-set)
* CopyKittens (intrusion-set)
* PROMETHIUM (intrusion-set)

## Affected Products

* cpe:2.3:a:honeywell:saia\_pg5\_controls\_suite:-:\*:\*:\*:\*:\*:\*:\*