# CVE Detail – CVE-2022-29959

Emerson OpenBSI through 2022-04-29 mishandles credential storage. It is an engineering environment for the ControlWave and Bristol Babcock line of RTUs. This environment provides access control functionality through user authentication and privilege management. The credentials for various users are stored insecurely in the SecUsers.ini file by using a simple string transformation rather than a cryptographic mechanism.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## EPSS

EPSS Score: N/A

Percentile: 0.15518

## CVSS Scoring

CVSS v3.1 Score: 5.5

Severity: MEDIUM

## Mapped CWE(s)

* CWE-522: Insufficiently Protected Credentials

## CAPEC(s)

* CAPEC-102: Session Sidejacking
* CAPEC-474: Signature Spoofing by Key Theft
* CAPEC-50: Password Recovery Exploitation
* CAPEC-509: Kerberoasting
* CAPEC-551: Modify Existing Service
* CAPEC-555: Remote Services with Stolen Credentials
* CAPEC-560: Use of Known Domain Credentials
* CAPEC-561: Windows Admin Shares with Stolen Credentials
* CAPEC-600: Credential Stuffing
* CAPEC-644: Use of Captured Hashes (Pass The Hash)
* CAPEC-645: Use of Captured Tickets (Pass The Ticket)
* CAPEC-652: Use of Known Kerberos Credentials
* CAPEC-653: Use of Known Operating System Credentials

## ATT&CK Techniques

* T1543: Create or Modify System Process
* T1133: External Remote Services
* T1558: Steal or Forge Kerberos Tickets
* T1021.002: SMB/Windows Admin Shares
* T1021: Remote Services
* T1552.004: Private Keys
* T1550.003: Pass the Ticket
* T1078: Valid Accounts
* T1110.004: Credential Stuffing
* T1114.002: Remote Email Collection
* T1550.002: Pass the Hash
* T1558.003: Kerberoasting

## Used By (Actors/Tools)

* TrickBot (malware)
* Stuxnet (malware)
* reGeorg (malware)
* Linux Rabbit (malware)
* Exaramel for Linux (malware)
* RansomHub (malware)
* LITTLELAMB.WOOLTEA (malware)
* IMAPLoader (malware)
* Emotet (malware)
* Olympic Destroyer (malware)
* BOLDMOVE (malware)
* BADHATCH (malware)
* Machete (malware)
* Mafalda (malware)
* Hildegard (malware)
* HOPLIGHT (malware)
* Regin (malware)
* Conti (malware)
* Diavol (malware)
* Doki (malware)
* Lucifer (malware)
* BlackEnergy (malware)
* zwShell (malware)
* NotPetya (malware)
* Conficker (malware)
* Anchor (malware)
* SeaDuke (malware)
* Duqu (malware)
* LightNeuron (malware)
* LockBit 3.0 (malware)
* FoggyWeb (malware)
* Royal (malware)
* Shamoon (malware)
* Akira \_v2 (malware)
* BlackByte Ransomware (malware)
* Ryuk (malware)
* LockBit 2.0 (malware)
* LunarMail (malware)
* Cobalt Strike (malware)
* Valak (malware)
* Kivars (malware)
* MacMa (malware)
* Kwampirs (malware)
* Troll Stealer (malware)
* Ebury (malware)
* Kinsing (malware)
* Industroyer (malware)
* jRAT (malware)
* Dtrack (malware)
* Zox (malware)
* Net Crawler (malware)
* HermeticWizard (malware)
* Net (tool)
* SILENTTRINITY (tool)
* PowerSploit (tool)
* Impacket (tool)
* AADInternals (tool)
* Empire (tool)
* PoshC2 (tool)
* Brute Ratel C4 (tool)
* MailSniper (tool)
* Pass-The-Hash Toolkit (tool)
* Mimikatz (tool)
* CrackMapExec (tool)
* Pupy (tool)
* Rubeus (tool)
* PsExec (tool)
* Indrik Spider (intrusion-set)
* C0027 (campaign)
* Operation Wocao (campaign)
* Wizard Spider (intrusion-set)
* FIN7 (intrusion-set)
* Velvet Ant (intrusion-set)
* ArcaneDoor (campaign)
* Dragonfly (intrusion-set)
* OilRig (intrusion-set)
* Fox Kitten (intrusion-set)
* SolarWinds Compromise (campaign)
* Lazarus Group (intrusion-set)
* Aquatic Panda (intrusion-set)
* Operation CuckooBees (campaign)
* Play (intrusion-set)
* Sandworm Team (intrusion-set)
* Turla (intrusion-set)
* Suckfly (intrusion-set)
* Ember Bear (intrusion-set)
* CostaRicto (campaign)
* TeamTNT (intrusion-set)
* FIN6 (intrusion-set)
* Silence (intrusion-set)
* APT28 (intrusion-set)
* Cinnamon Tempest (intrusion-set)
* Ke3chang (intrusion-set)
* Volt Typhoon (intrusion-set)
* Leafminer (intrusion-set)
* Magic Hound (intrusion-set)
* APT29 (intrusion-set)
* 2016 Ukraine Electric Power Attack (campaign)
* HAFNIUM (intrusion-set)
* APT39 (intrusion-set)
* APT32 (intrusion-set)
* BRONZE BUTLER (intrusion-set)
* POLONIUM (intrusion-set)
* Kimsuky (intrusion-set)
* Leviathan (intrusion-set)
* Storm-1811 (intrusion-set)
* Akira (intrusion-set)
* LAPSUS$ (intrusion-set)
* Chimera (intrusion-set)
* ToddyCat (intrusion-set)
* menuPass (intrusion-set)
* 2015 Ukraine Electric Power Attack (campaign)
* Moses Staff (intrusion-set)
* Threat Group-1314 (intrusion-set)
* APT41 (intrusion-set)
* INC Ransom (intrusion-set)
* FIN13 (intrusion-set)
* GALLIUM (intrusion-set)
* FIN10 (intrusion-set)
* FIN8 (intrusion-set)
* Rocke (intrusion-set)
* Scattered Spider (intrusion-set)
* Blue Mockingbird (intrusion-set)
* FIN4 (intrusion-set)
* BlackByte (intrusion-set)
* Threat Group-3390 (intrusion-set)
* APT28 Nearest Neighbor Campaign (campaign)
* Night Dragon (campaign)
* Sea Turtle (intrusion-set)
* Leviathan Australian Intrusions (campaign)
* Axiom (intrusion-set)
* APT3 (intrusion-set)
* Operation MidnightEclipse (campaign)
* C0032 (campaign)
* APT1 (intrusion-set)
* HomeLand Justice (campaign)
* FIN5 (intrusion-set)
* APT33 (intrusion-set)
* Cutting Edge (campaign)
* GOLD SOUTHFIELD (intrusion-set)
* Silent Librarian (intrusion-set)
* APT18 (intrusion-set)
* Carbanak (intrusion-set)
* Orangeworm (intrusion-set)
* Deep Panda (intrusion-set)
* Star Blizzard (intrusion-set)
* PittyTiger (intrusion-set)

## Affected Products

* cpe:2.3:a:emerson:openbsi:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:emerson:openbsi:5.9:-:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:emerson:openbsi:5.9:sp1:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:emerson:openbsi:5.9:sp2:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:emerson:openbsi:5.9:sp3:\*:\*:\*:\*:\*:\*