# CVE Detail – CVE-2022-29965

The Emerson DeltaV Distributed Control System (DCS) controllers and IO cards through 2022-04-29 misuse passwords. Access to privileged operations on the maintenance port TELNET interface (23/TCP) on M-series and SIS (CSLS/LSNB/LSNG) nodes is controlled by means of utility passwords. These passwords are generated using a deterministic, insecure algorithm using a single seed value composed of a day/hour/minute timestamp with less than 16 bits of entropy. The seed value is fed through a lookup table and a series of permutation operations resulting in three different four-character passwords corresponding to different privilege levels. An attacker can easily reconstruct these passwords and thus gain access to privileged maintenance operations. NOTE: this is different from CVE-2014-2350.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## EPSS

EPSS Score: N/A

Percentile: 0.04107

## CVSS Scoring

CVSS v3.1 Score: 5.5

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:emerson:deltav\_distributed\_control\_system:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:emerson:deltav\_distributed\_control\_system\_sq\_controller\_firmware:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:emerson:deltav\_distributed\_control\_system\_sx\_controller\_firmware:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:emerson:se4002s1t2b6\_high\_side\_40-pin\_mass\_i\/o\_terminal\_block\_firmware:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:emerson:se4003s2b4\_16-pin\_mass\_i\/o\_terminal\_block\_firmware:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:emerson:se4003s2b524-pin\_mass\_i\/o\_terminal\_block\_firmware:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:emerson:se4017p0\_h1\_i\/o\_interface\_card\_and\_terminl\_block\_firmware:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:emerson:se4017p1\_h1\_i\/o\_card\_with\_integrated\_power\_firmware:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:emerson:se4019p0\_simplex\_h1\_4-port\_plus\_fieldbus\_i\/o\_interface\_with\_terminalblock\_firmware:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:emerson:se4026\_virtual\_i\/o\_module\_2\_firmware:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:emerson:se4027\_virtual\_i\/o\_module\_2\_firmware:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:emerson:se4032s1t2b8\_high\_side\_40-pin\_do\_mass\_i\/o\_terminal\_block\_firmware:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:emerson:se4037p0\_h1\_i\/o\_interface\_card\_and\_terminl\_block\_firmware:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:emerson:se4037p1\_redundant\_h1\_i\/o\_card\_with\_integrated\_power\_and\_terminal\_block\_firmware:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:emerson:se4039p0\_redundant\_h1\_4-port\_plus\_fieldbus\_i\/o\_interface\_with\_terminalblock\_firmware:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:emerson:se4052s1t2b6\_high\_side\_40-pin\_mass\_i\/o\_terminal\_block\_firmware:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:emerson:se4082s1t2b8\_high\_side\_40-pin\_do\_mass\_i\/o\_terminal\_block\_firmware:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:emerson:se4100\_simplex\_ethernet\_i\/o\_card\_\(eioc\)\_assembly\_firmware:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:emerson:se4101\_simplex\_ethernet\_i\/o\_card\_\(eioc\)\_assembly\_firmware:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:emerson:se4801t0x\_redundant\_wireless\_i\/o\_card\_firmware:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:emerson:ve4103\_modbus\_tcp\_interface\_for\_ethernet\_connected\_i\/o\_\(eioc\)\_firmware:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:emerson:ve4104\_ethernet\/ip\_control\_tag\_integration\_for\_ethernet\_connected\_i\/o\_\(eioc\)\_firmware:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:emerson:ve4105\_ethernet\/ip\_interface\_for\_ethernet\_connected\_i\/o\_\(eioc\)\_firmware:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:emerson:ve4106\_opc-ua\_client\_for\_ethernet\_connected\_i\/o\_\(eioc\)\_firmware:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:emerson:ve4107\_iec\_61850\_mms\_interface\_for\_ethernet\_connected\_i\/o\_\(eioc\)\_firmware:\*:\*:\*:\*:\*:\*:\*:\*