# CVE Detail – CVE-2022-29964

The Emerson DeltaV Distributed Control System (DCS) controllers and IO cards through 2022-04-29 misuse passwords. WIOC SSH provides access to a shell as root, DeltaV, or backup via hardcoded credentials. NOTE: this is different from CVE-2014-2350.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## EPSS

EPSS Score: N/A

Percentile: 0.07262

## CVSS Scoring

CVSS v3.1 Score: 5.5

Severity: MEDIUM

## Mapped CWE(s)

* CWE-798: Use of Hard-coded Credentials

## CAPEC(s)

* CAPEC-191: Read Sensitive Constants Within an Executable
* CAPEC-70: Try Common or Default Usernames and Passwords

## ATT&CK Techniques

* T1078.001: Default Accounts
* T1552.001: Credentials In Files

## Used By (Actors/Tools)

* TrickBot (malware)
* Stuxnet (malware)
* Smoke Loader (malware)
* HyperStack (malware)
* Emotet (malware)
* Hildegard (malware)
* BlackEnergy (malware)
* XTunnel (malware)
* pngdowner (malware)
* StrelaStealer (malware)
* Pysa (malware)
* Agent Tesla (malware)
* jRAT (malware)
* Azorult (malware)
* AADInternals (tool)
* Empire (tool)
* PoshC2 (tool)
* LaZagne (tool)
* Pupy (tool)
* QuasarRAT (tool)
* Indrik Spider (intrusion-set)
* OilRig (intrusion-set)
* Fox Kitten (intrusion-set)
* TA505 (intrusion-set)
* Ember Bear (intrusion-set)
* TeamTNT (intrusion-set)
* Leafminer (intrusion-set)
* Magic Hound (intrusion-set)
* MuddyWater (intrusion-set)
* Kimsuky (intrusion-set)
* FIN13 (intrusion-set)
* Scattered Spider (intrusion-set)
* RedCurl (intrusion-set)
* Leviathan Australian Intrusions (campaign)
* APT3 (intrusion-set)
* HomeLand Justice (campaign)
* APT33 (intrusion-set)

## Affected Products

* 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:\*:\*:\*:\*:\*:\*:\*:\*