# CVE Detail – CVE-2022-30260

Emerson DeltaV Distributed Control System (DCS) has insufficient verification of firmware integrity (an inadequate checksum approach, and no signature). This affects versions before 14.3 of DeltaV M-series, DeltaV S-series, DeltaV P-series, DeltaV SIS, and DeltaV CIOC/EIOC/WIOC IO cards.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## EPSS

EPSS Score: N/A

Percentile: 0.05819

## CVSS Scoring

CVSS v3.1 Score: 7.8

Severity: HIGH

## Mapped CWE(s)

* CWE-345: Insufficient Verification of Data Authenticity

## CAPEC(s)

* CAPEC-111: JSON Hijacking (aka JavaScript Hijacking)
* CAPEC-141: Cache Poisoning
* CAPEC-142: DNS Cache Poisoning
* CAPEC-148: Content Spoofing
* CAPEC-218: Spoofing of UDDI/ebXML Messages
* CAPEC-384: Application API Message Manipulation via Man-in-the-Middle
* CAPEC-385: Transaction or Event Tampering via Application API Manipulation
* CAPEC-386: Application API Navigation Remapping
* CAPEC-387: Navigation Remapping To Propagate Malicious Content
* CAPEC-388: Application API Button Hijacking
* CAPEC-665: Exploitation of Thunderbolt Protection Flaws
* CAPEC-701: Browser in the Middle (BiTM)

## ATT&CK Techniques

* T1491: Defacement
* T1542.002: Component Firmware
* T1584.002: DNS Server
* T1557.002: ARP Cache Poisoning
* T1556: Modify Authentication Process
* T1211: Exploitation for Defense Evasion

## Used By (Actors/Tools)

* Cyclops Blink (malware)
* Kessel (malware)
* Ebury (malware)
* SILENTTRINITY (tool)
* LuminousMoth (intrusion-set)
* Velvet Ant (intrusion-set)
* ArcaneDoor (campaign)
* Equation (intrusion-set)
* APT28 (intrusion-set)
* LAPSUS$ (intrusion-set)
* FIN13 (intrusion-set)
* Sea Turtle (intrusion-set)
* Cleaver (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:\*:\*:\*:\*:\*:\*:\*:\*