# CVE Detail – CVE-2022-31204

Omron CS series, CJ series, and CP series PLCs through 2022-05-18 use cleartext passwords. They feature a UM Protection setting that allows users or system integrators to configure a password in order to restrict sensitive engineering operations (such as project/logic uploads and downloads). This password is set using the OMRON FINS command Program Area Protect and unset using the command Program Area Protect Clear, both of which are transmitted in cleartext.

## Threat-Mapped Scoring

Score: 3.0

Priority: P2 - Serious (High)

## EPSS

EPSS Score: N/A

Percentile: 0.29362

## CVSS Scoring

CVSS v3.1 Score: 7.5

Severity: HIGH

## Mapped CWE(s)

* CWE-319: Cleartext Transmission of Sensitive Information

## CAPEC(s)

* CAPEC-102: Session Sidejacking
* CAPEC-117: Interception
* CAPEC-383: Harvesting Information via API Event Monitoring
* CAPEC-477: Signature Spoofing by Mixing Signed and Unsigned Content
* CAPEC-65: Sniff Application Code

## ATT&CK Techniques

* T1040: Network Sniffing
* T1056.004: Credential API Hooking

## Used By (Actors/Tools)

* TrickBot (malware)
* cd00r (malware)
* JumbledPath (malware)
* RDFSNIFFER (malware)
* NOKKI (malware)
* VersaMem (malware)
* Ursnif (malware)
* Zeus Panda (malware)
* J-magic (malware)
* Emotet (malware)
* Regin (malware)
* Line Dancer (malware)
* FoggyWeb (malware)
* MESSAGETAP (malware)
* Zebrocy (malware)
* FinFisher (malware)
* Carberp (malware)
* ZxShell (malware)
* Penquin (malware)
* Impacket (tool)
* Empire (tool)
* PoshC2 (tool)
* Responder (tool)
* NBTscan (tool)
* Velvet Ant (intrusion-set)
* ArcaneDoor (campaign)
* Sandworm Team (intrusion-set)
* APT28 (intrusion-set)
* Kimsuky (intrusion-set)
* 2015 Ukraine Electric Power Attack (campaign)
* DarkVishnya (intrusion-set)
* PLATINUM (intrusion-set)
* Salt Typhoon (intrusion-set)
* APT33 (intrusion-set)

## Affected Products

* cpe:2.3:o:omron:sysmac\_cs1\_firmware:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:omron:sysmac\_cj2m\_firmware:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:omron:sysmac\_cj2h\_firmware:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:omron:sysmac\_cp1e\_firmware:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:omron:sysmac\_cp1h\_firmware:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:omron:sysmac\_cp1l\_firmware:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:omron:cp1w-cif41\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:omron:cx-programmer:\*:\*:\*:\*:\*:\*:\*:\*