INCONTROLLER, Software S1045 | MITRE ATT&CK®

ICS T0858 Change Operating Mode

INCONTROLLER can establish a remote HTTP connection to change the operating mode of Omron PLCs.[3][5]

ICS T0884 Connection Proxy

The INCONTROLLER PLCProxy module can add an IP route to the CODESYS gateway running on Schneider PLCs to allow it to route messages through the PLC to other devices on that network. This allows the malware to bypass firewall rules that prevent it from directly communicating with devices on the same network as the PLC.[5]

ICS T0809 Data Destruction

INCONTROLLER can wipe the memory of Omron PLCs and reset settings through the remote HTTP service.[2][3][5]

ICS T0890 Exploitation for Privilege Escalation

INCONTROLLER has the ability to exploit a vulnerable Asrock driver (AsrDrv103.sys) using CVE-2020-15368 to load its own unsigned driver on the system.[5]

ICS T0891 Hardcoded Credentials

INCONTROLLER can login to Omron PLCs using hardcoded credentials, which is documented in CVE-2022-34151.[5]

ICS T0867 Lateral Tool Transfer

INCONTROLLER can use a Telnet session to load a malware implant on Omron PLCs.[1][5]

ICS T0836 Modify Parameter

INCONTROLLER can use the HTTP CGI scripts on Omron PLCs to modify parameters on EtherCat connected servo drives.[5]

ICS T0842 Network Sniffing

INCONTROLLER can deploy Tcpdump to sniff network traffic and collect PCAP files.[5]

ICS T0861 Point & Tag Identification

INCONTROLLER can remotely read the OCP UA structure from devices.[1]

ICS T0843 Program Download

INCONTROLLER can use the CODESYS protocol to download programs to Schneider PLCs.[5][2]

INCONTROLLER can modified program logic on Omron PLCs using either the program download or backup transfer functions available through the HTTP server.[5]

ICS T0845 Program Upload

INCONTROLLER can use the CODESYS protocol to upload programs from Schneider PLCs.[5][2]

INCONTROLLER can obtain existing program logic from Omron PLCs by using either the program upload or backup functions available through the HTTP server.[5]

ICS T0886 Remote Services

INCONTROLLER can use the CODESYS protocol to remotely connect to Schneider PLCs and perform maintenance functions on the device.[5]

INCONTROLLER can use Telnet to upload payloads and execute commands on Omron PLCs. [2][3] The malware can also use HTTP-based CGI scripts (e.g., cpu.fcgi, ecat.fcgi) to gain administrative access to the device.[5]

ICS T0846 Remote System Discovery

INCONTROLLER can perform a UDP multicast scan of UDP port 27127 to identify Schneider PLCs that use that port for the NetManage protocol.[3][5]

INCONTROLLER can use the FINS (Factory Interface Network Service) protocol to scan for and obtain MAC address associated with Omron devices.[1][5]

INCONTROLLER has the ability to perform scans for TCP port 4840 to identify devices running OPC UA servers.[5]

ICS T0888 Remote System Information Discovery

INCONTROLLER includes a library that creates Modbus connections with a device to request its device ID.[1][5]

ICS T0869 Standard Application Layer Protocol

INCONTROLLER can remotely send commands to a malicious agent uploaded on Omron PLCs over HTTP or HTTPS.[1]

ICS T0855 Unauthorized Command Message

INCONTROLLER can send custom Modbus commands to write register values on Schneider PLCs.[1]

INCONTROLLER can send write tag values on OPC UA servers.[1]

ICS T0859 Valid Accounts

INCONTROLLER can brute force password-based authentication to Schneider PLCs over the CODESYS protocol (UDP port 1740).[1]

INCONTROLLER can perform brute force guessing of passwords to OPC UA servers using a predefined list of passwords.[1][5]
