Grid-SIEM

Fall 2023 | Group 29 | CPRE 491

Project Update

- Gravwell Meeting
- Gravwell Installation Updates
- Security Onion Updates
- Protocols in MITRE Caldera
- Questions?

Gravwell

- New resources to research provided in Gravwell demo meeting such as Kits. Best resource moving forward would be discord channel. Speaking directly to devs.
- Gravwell has been installed from Debian repo. Using file follower ingester. File Follow will automatically ingest standard Linux log (i.e. /var/log/).
- Where should we feed the data in from?
- One machine only?
- Next steps: Set up Zeek collection logs to gain visibility into network traffic.

Gravwell: Tags and Flow

- Tags
  - Syslog, sysmon, tor, http, etc.
  - tag=pcap packet modbus.Function modbus.Unit modbus.Length modbus.Protocol modbus.Transaction modbus.Payload ipv4.SrcIP ipv4.DstIP | hexlify Payload | table SrcIP DstIP Protocol Unit Transaction Length Function Payload
    - Very long, but checks all pcap packets for modbus protocol
- Flow
  - Automatically run a search query and then do x with it
    - Email, run through python, log
  - Can send same data through multiple "flows"
    - This means we can tailor our parsed logs in a format for SIEMS and a format for ML at the same time

Security Onion

- Going through the configuration
- Questions:
  - Did the IPs or interfaces change?
  - Were there any firewall rules that needed to be adjusted on the firewall VMs?
  - When trying to setup another sensor, still having connectivity issues, how was it fixed on the new sensor?

Protocols in MITRE Caldera

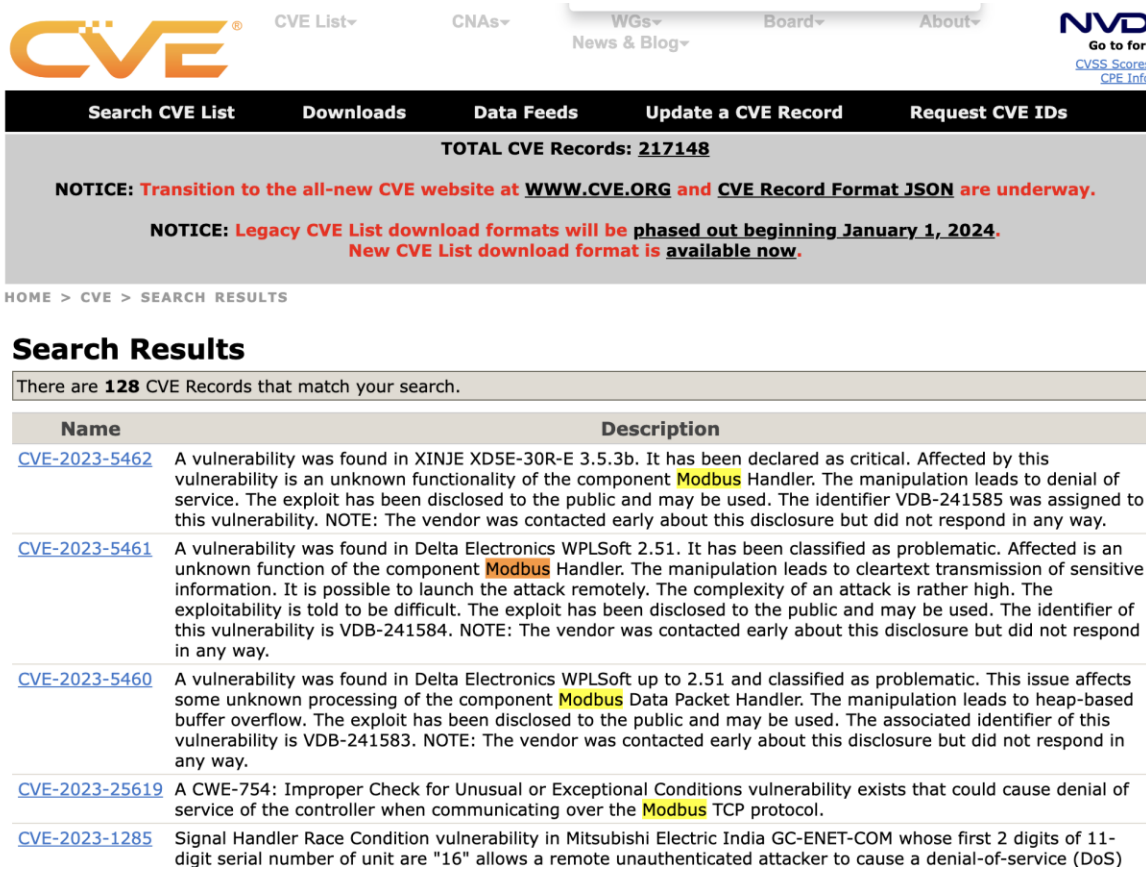
- Bacnet, dnp3, and modbus plugins are installed on Caldera instance on the kali VM
- Clarification on where dnp3 is used
- Caldera documentation states that payloads are a list of files needed for attack to run

tion							
DOS/DDOS	TCP/ICMP		Non-Modbus traffic	Stealthy/Not Stealthy	IDS Rules	Yes	Medium
	Modbus	Illegal address - Write	Write req. on Modbus coil	Stealthy	IDS Rules and Blacklisting	Yes	High
Modbus Function Code	Modbus	Read	Coil	Stealthy	IDS Rules and Blacklisting	Yes	Low
	Modbus	Read	Holding register	Stealthy	IDS Rules and Blacklisting	Yes	Low
	Modbus	Read	Discrete input	Stealthy	IDS Rules and Blacklisting	Yes	Low
	Modbus	Read	Input register	Stealthy	IDS Rules and Blacklisting	Yes	Low
	Modbus	Write	Coil	Stealthy	IDS Rules and Blacklisting	Yes	High
	Modbus	Write	Holding register	Stealthy	IDS Rules and Blacklisting	Yes	High
	Modbus	Write/Read	Holding register check data	Stealthy	IDS Rules	Yes	High

Modbus Vulnerabilities & Payloads

- Many Modbus vulnerabilities on Mitre CVE list
  - 128
  - Example: CVE-2022-30938
    - A vulnerability has been identified in EN100 Ethernet module DNP3 IP variant (All versions), EN100 Ethernet module IEC 104 variant (All versions), EN100 Ethernet module IEC 61850 variant (All versions < V4.40), EN100 Ethernet module Modbus TCP variant (All versions), EN100 Ethernet module PROFINET IO variant (All versions)
    - https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=modbus
- Modbus payloads:

  Found multiple payloads on the Metasploit git page
  - Modbus banner grabbing
  - Modbus find unit id
  - Modbus client
  - Modbus detect
  - https://github.com/rapid7/metasploit-framework/blob/master/modules/auxiliary/scanner/scada/modbus_banner_grabbing.rb



CVE List CNAs WGs Board About News & Blog

Search CVE List | Downloads | Data Feeds | Update a CVE Record | Request CVE IDs

TOTAL CVE Records: 217148

NOTICE: Transition to the all-new CVE website at WWW.CVE.ORG and CVE Record Format JSON are underway.

NOTICE: Legacy CVE List download formats will be phased out beginning January 1, 2024.
New CVE List download format is available now.

HOME > CVE > SEARCH RESULTS

Search Results

There are **128** CVE Records that match your search.

Name	Description
CVE-2023-5462	A vulnerability was found in XINJE XD5E-30R-E 3.5.3b. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the component Modbus Handler. The manipulation leads to denial of service. The exploit has been disclosed to the public and may be used. The identifier VDB-241585 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.
CVE-2023-5461	A vulnerability was found in Delta Electronics WPLSoft 2.51. It has been classified as problematic. Affected is an unknown function of the component Modbus Handler. The manipulation leads to cleartext transmission of sensitive information. It is possible to launch the attack remotely. The complexity of an attack is rather high. The exploitability is told to be difficult. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-241584. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.
CVE-2023-5460	A vulnerability was found in Delta Electronics WPLSoft up to 2.51 and classified as problematic. This issue affects some unknown processing of the component Modbus Data Packet Handler. The manipulation leads to heap-based buffer overflow. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-241583. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.
CVE-2023-25619	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists that could cause denial of service of the controller when communicating over the Modbus TCP protocol.
CVE-2023-1285	Signal Handler Race Condition vulnerability in Mitsubishi Electric India GC-ENET-COM whose first 2 digits of 11-digit serial number of unit are "16" allows a remote unauthenticated attacker to cause a denial-of-service (DoS)

Coming Up

- Polished draft of project documentation.
- Update the team website.
- Turn in the YouTube video and weekly report 5.
- Use Kali VM to attack SIEM defenses
- Produce a PowerCyber infrastructure overview for final presentation faculty panel.
- Explore PyTorch or TensorFlow ML options.