Leveraging AI for Automated Attack Vector Extraction and Vulnerability Prevention

Patrick Kuo, Threat Research Manager
Daniel Chiu, Threat Research Manager
Canaan Kao, Threat Research Director

Threat Research, TXOne Networks Inc.

March 17, 2025 @CYBERSEC 2025

Speakers

- Patrick 目前任職於TXOne Networks 的Threat Research Team Manager，主要開發的系統為Threat Hunting System，Threat Hunting Agent以及Threat Atlas。曾在BalckHat Europe，FIRST，CyberSEC以及HitCon擔任講師。目前主要任務是帶領團隊研究惡意軟體偵測，資料分析，漏洞評估以及核心系統架構以及模組的開發。

- Daniel Chiu 任職於 TXOne Networks，擔任Threat Signature Research Team Manager，自2013就業以來專注在DPI的改進和DPI特徵碼的撰寫，目前帶領團隊分析網路漏洞、開發IPS rule和ICS Protocol相關研究。
- 興趣:研究網路攻擊手法和改進防禦方法。

- Canaan 自 2001 年起擔任 DPI/IDS/IPS 工程師。他領導了 MoECC 委託給 NTHU 的 Anti-Botnet 計畫（2009 - 2013）並舉辦了 “Botnet of Taiwan”（BoT）研討會（2009 - 2014）。他在 HitCon2014 CMT、HitCon2015 CMT 和 HitCon 2019 發表過演講。他目前任職於 TXOne 擔任 Threat Research 部門的主管。他的主要研究興趣是網路安全、入侵偵測系統、逆向工程、惡意軟體偵測和嵌入式系統。

Outline

01 | **Understand vulnerability assessment**

02 | **Vulnerability lifecycle pipeline**

03 | **Automated extraction attack patterns**

04 | **Vulnerability prevention flowchart**

05 | **Benefits of vulnerability prevention**

06 | **Vulnerability prevention demonstration**

Understand vulnerability assessment

Understanding vulnerability assessment

- Vulnerability assessment is in cybersecurity to identify and prioritize system weaknesses.
- According to detect asset information, vulnerability assessment can disclose the threat of the asset and highlight the compromised risk of asset.

Ur

Security recommendations > txone-webinspec

[redacted]

No known risks Criticality: None

Overview | Incidents and alerts | Timeline | Security policies | Security recommendations | Inventories | Discovered vulnerabilities | Missing KBs

VM details

Category
Computers and Mobile

Type
Unknown

Subtype
Workstation

Discovery sources

Domain
AAD joined

OS
Windows 10 WVD 64-bit (Release 22H2 Build 19045.5131)

SAM name
-

Health state
Inactive

Data sensitivity
None

[redacted]

MAC address
-

Last seen
Mar 5, 2025 11:32:50 AM

Onboarding status
Onboarded

Resources
-

Asset group
-

[redacted]

Active alerts (Last 180 days)

No active alerts or incidents

Security assessments

Exposure level: High

67 active security recommendations

Discovered vulnerabilities (244)

Critical (3) High (142) 2 more

View all recommendations

Logged on users (Last 30 days)

1 logged on user

[redacted]

View 1 logged on user

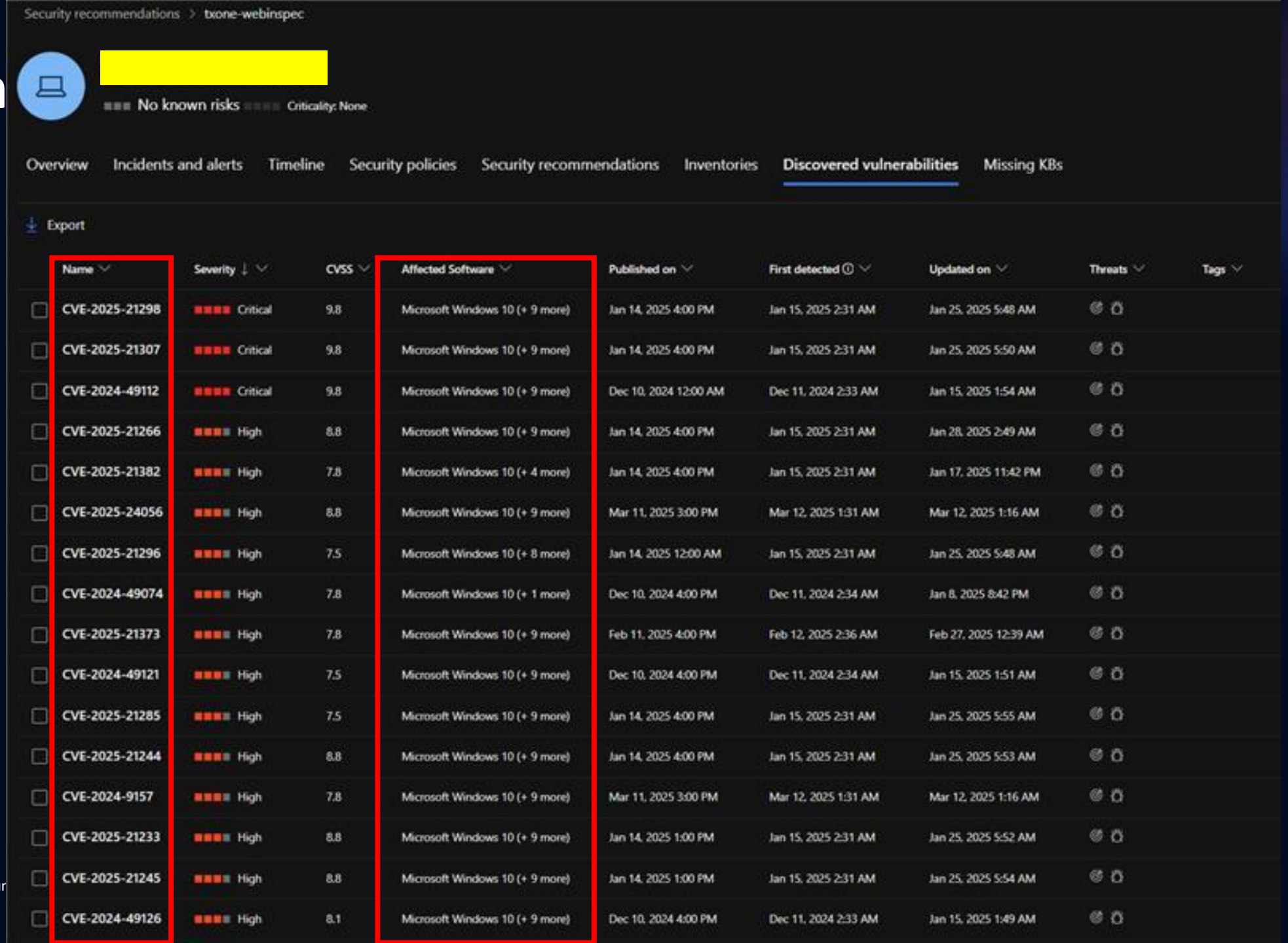
Device health status

Security intelligence update status is unknown +3 more issues

Type	State	Date & time
Last full scan	No scan performed	
Last quick scan	Completed	Mar 4, 2025 5:09:25 ...
Security intelligence	Version 1.423.220.0	Mar 4, 2025 9:41:48 ...
Engine	Version 1.1.25010.7	Mar 4, 2025 9:41:49 ...
Platform	Version 4.18.24090.11	Nov 12, 2024 2:56:2...

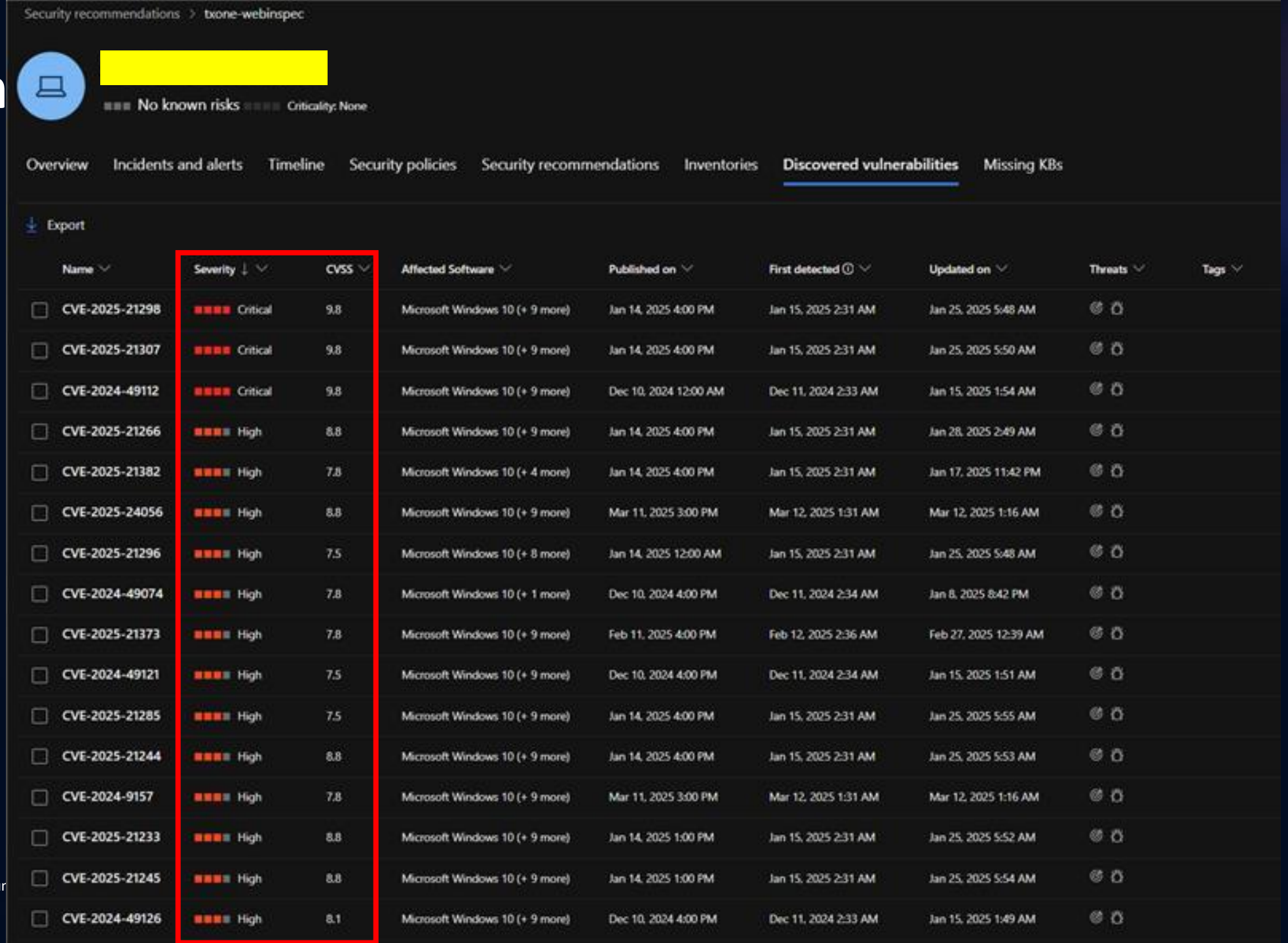
txOne networks

Un



Name	Severity	CVSS	Affected Software	Published on	First detected	Updated on	Threats	Tags
CVE-2025-21298	Critical	9.8	Microsoft Windows 10 (+ 9 more)	Jan 14, 2025 4:00 PM	Jan 15, 2025 2:31 AM	Jan 25, 2025 5:48 AM		
CVE-2025-21307	Critical	9.8	Microsoft Windows 10 (+ 9 more)	Jan 14, 2025 4:00 PM	Jan 15, 2025 2:31 AM	Jan 25, 2025 5:50 AM		
CVE-2024-49112	Critical	9.8	Microsoft Windows 10 (+ 9 more)	Dec 10, 2024 12:00 AM	Dec 11, 2024 2:33 AM	Jan 15, 2025 1:54 AM		
CVE-2025-21266	High	8.8	Microsoft Windows 10 (+ 9 more)	Jan 14, 2025 4:00 PM	Jan 15, 2025 2:31 AM	Jan 28, 2025 2:49 AM		
CVE-2025-21382	High	7.8	Microsoft Windows 10 (+ 4 more)	Jan 14, 2025 4:00 PM	Jan 15, 2025 2:31 AM	Jan 17, 2025 11:42 PM		
CVE-2025-24056	High	8.8	Microsoft Windows 10 (+ 9 more)	Mar 11, 2025 3:00 PM	Mar 12, 2025 1:31 AM	Mar 12, 2025 1:16 AM		
CVE-2025-21296	High	7.5	Microsoft Windows 10 (+ 8 more)	Jan 14, 2025 12:00 AM	Jan 15, 2025 2:31 AM	Jan 25, 2025 5:48 AM		
CVE-2024-49074	High	7.8	Microsoft Windows 10 (+ 1 more)	Dec 10, 2024 4:00 PM	Dec 11, 2024 2:34 AM	Jan 8, 2025 8:42 PM		
CVE-2025-21373	High	7.8	Microsoft Windows 10 (+ 9 more)	Feb 11, 2025 4:00 PM	Feb 12, 2025 2:36 AM	Feb 27, 2025 12:39 AM		
CVE-2024-49121	High	7.5	Microsoft Windows 10 (+ 9 more)	Dec 10, 2024 4:00 PM	Dec 11, 2024 2:34 AM	Jan 15, 2025 1:51 AM		
CVE-2025-21285	High	7.5	Microsoft Windows 10 (+ 9 more)	Jan 14, 2025 4:00 PM	Jan 15, 2025 2:31 AM	Jan 25, 2025 5:55 AM		
CVE-2025-21244	High	8.8	Microsoft Windows 10 (+ 9 more)	Jan 14, 2025 4:00 PM	Jan 15, 2025 2:31 AM	Jan 25, 2025 5:53 AM		
CVE-2024-9157	High	7.8	Microsoft Windows 10 (+ 9 more)	Mar 11, 2025 3:00 PM	Mar 12, 2025 1:31 AM	Mar 12, 2025 1:16 AM		
CVE-2025-21233	High	8.8	Microsoft Windows 10 (+ 9 more)	Jan 14, 2025 1:00 PM	Jan 15, 2025 2:31 AM	Jan 25, 2025 5:52 AM		
CVE-2025-21245	High	8.8	Microsoft Windows 10 (+ 9 more)	Jan 14, 2025 1:00 PM	Jan 15, 2025 2:31 AM	Jan 25, 2025 5:54 AM		
CVE-2024-49126	High	8.1	Microsoft Windows 10 (+ 9 more)	Dec 10, 2024 4:00 PM	Dec 11, 2024 2:33 AM	Jan 15, 2025 1:49 AM		

Un



Name	Severity	CVSS	Affected Software	Published on	First detected	Updated on	Threats	Tags
CVE-2025-21298	Critical	9.8	Microsoft Windows 10 (+ 9 more)	Jan 14, 2025 4:00 PM	Jan 15, 2025 2:31 AM	Jan 25, 2025 5:48 AM		
CVE-2025-21307	Critical	9.8	Microsoft Windows 10 (+ 9 more)	Jan 14, 2025 4:00 PM	Jan 15, 2025 2:31 AM	Jan 25, 2025 5:50 AM		
CVE-2024-49112	Critical	9.8	Microsoft Windows 10 (+ 9 more)	Dec 10, 2024 12:00 AM	Dec 11, 2024 2:33 AM	Jan 15, 2025 1:54 AM		
CVE-2025-21266	High	8.8	Microsoft Windows 10 (+ 9 more)	Jan 14, 2025 4:00 PM	Jan 15, 2025 2:31 AM	Jan 28, 2025 2:49 AM		
CVE-2025-21382	High	7.8	Microsoft Windows 10 (+ 4 more)	Jan 14, 2025 4:00 PM	Jan 15, 2025 2:31 AM	Jan 17, 2025 11:42 PM		
CVE-2025-24056	High	8.8	Microsoft Windows 10 (+ 9 more)	Mar 11, 2025 3:00 PM	Mar 12, 2025 1:31 AM	Mar 12, 2025 1:16 AM		
CVE-2025-21296	High	7.5	Microsoft Windows 10 (+ 8 more)	Jan 14, 2025 12:00 AM	Jan 15, 2025 2:31 AM	Jan 25, 2025 5:48 AM		
CVE-2024-49074	High	7.8	Microsoft Windows 10 (+ 1 more)	Dec 10, 2024 4:00 PM	Dec 11, 2024 2:34 AM	Jan 8, 2025 8:42 PM		
CVE-2025-21373	High	7.8	Microsoft Windows 10 (+ 9 more)	Feb 11, 2025 4:00 PM	Feb 12, 2025 2:36 AM	Feb 27, 2025 12:39 AM		
CVE-2024-49121	High	7.5	Microsoft Windows 10 (+ 9 more)	Dec 10, 2024 4:00 PM	Dec 11, 2024 2:34 AM	Jan 15, 2025 1:51 AM		
CVE-2025-21285	High	7.5	Microsoft Windows 10 (+ 9 more)	Jan 14, 2025 4:00 PM	Jan 15, 2025 2:31 AM	Jan 25, 2025 5:55 AM		
CVE-2025-21244	High	8.8	Microsoft Windows 10 (+ 9 more)	Jan 14, 2025 4:00 PM	Jan 15, 2025 2:31 AM	Jan 25, 2025 5:53 AM		
CVE-2024-9157	High	7.8	Microsoft Windows 10 (+ 9 more)	Mar 11, 2025 3:00 PM	Mar 12, 2025 1:31 AM	Mar 12, 2025 1:16 AM		
CVE-2025-21233	High	8.8	Microsoft Windows 10 (+ 9 more)	Jan 14, 2025 1:00 PM	Jan 15, 2025 2:31 AM	Jan 25, 2025 5:52 AM		
CVE-2025-21245	High	8.8	Microsoft Windows 10 (+ 9 more)	Jan 14, 2025 1:00 PM	Jan 15, 2025 2:31 AM	Jan 25, 2025 5:54 AM		
CVE-2024-49126	High	8.1	Microsoft Windows 10 (+ 9 more)	Dec 10, 2024 4:00 PM	Dec 11, 2024 2:33 AM	Jan 15, 2025 1:49 AM		

txOne networks

Understanding vulnerability assessment

- The process involves asset discovery, scanning for vulnerabilities, assessment, remediation information and fix identified risks.

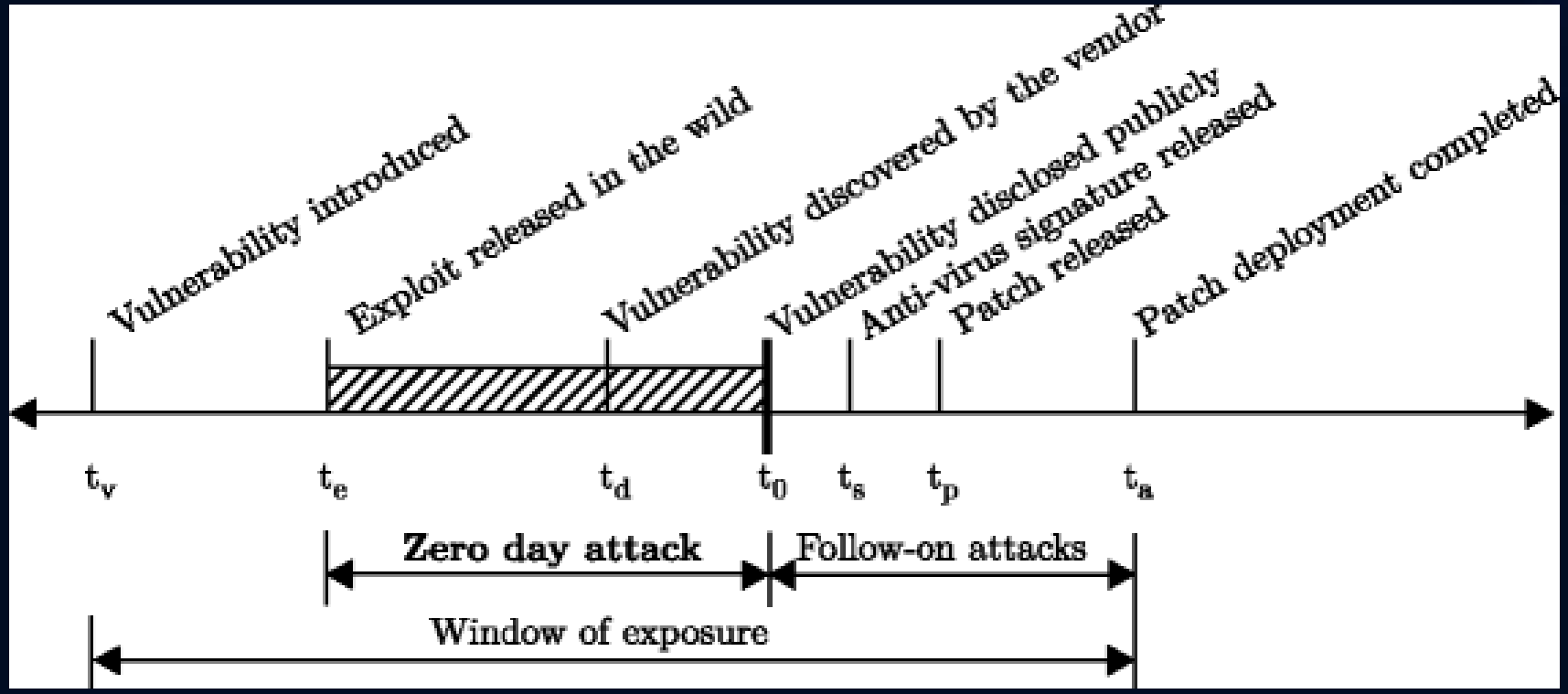
Reference from
[https://www.microsoft.com/zh-tw/security/business/threat-protection/microsoft-defender-vulnerability-management]

Understanding vulnerability assessment

- And in the most scenarios, **remediation and fix processes** can't be implemented easily.
- For a **0day** vulnerability, it's fixed or mitigated **until the patch is released and installed into the asset**. The period of the time will be longer.
- In early stage of vulnerability assessment, implementing the LLM model can decrease the risk which is about the asset is compromised.

Vulnerability lifecycle pipeline

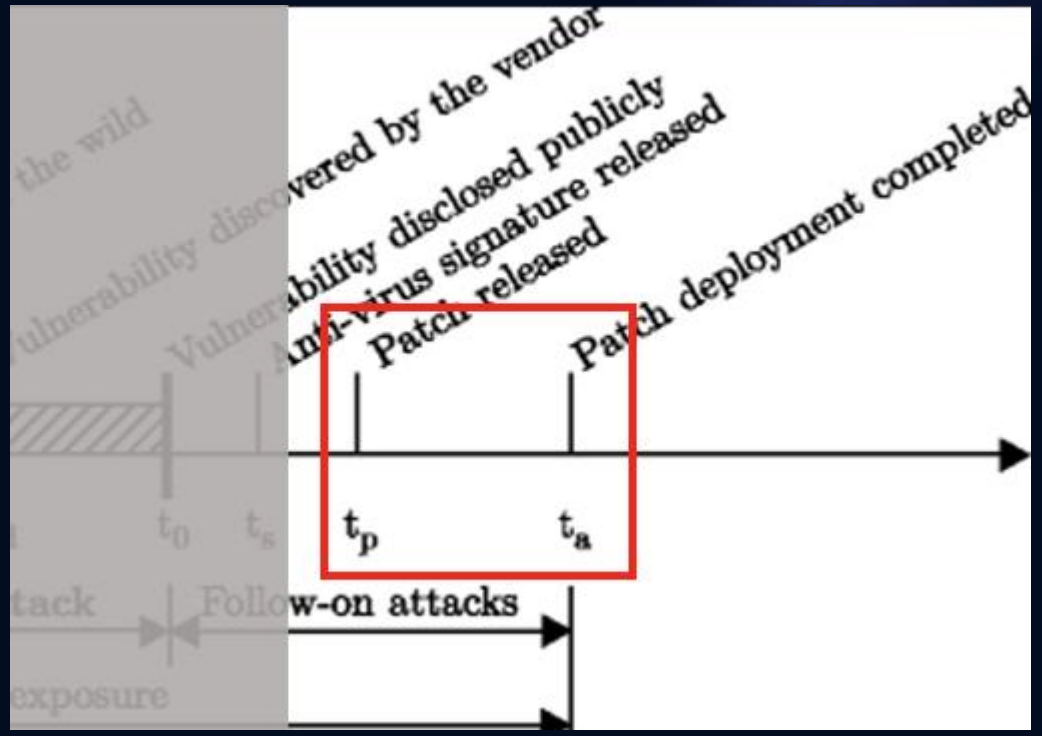
Vulnerability lifecycle pipeline



Reference from
[https://www.researchgate.net/figure/The-attack-timeline-for-zero-day-attacks-12_fig3_323858550]

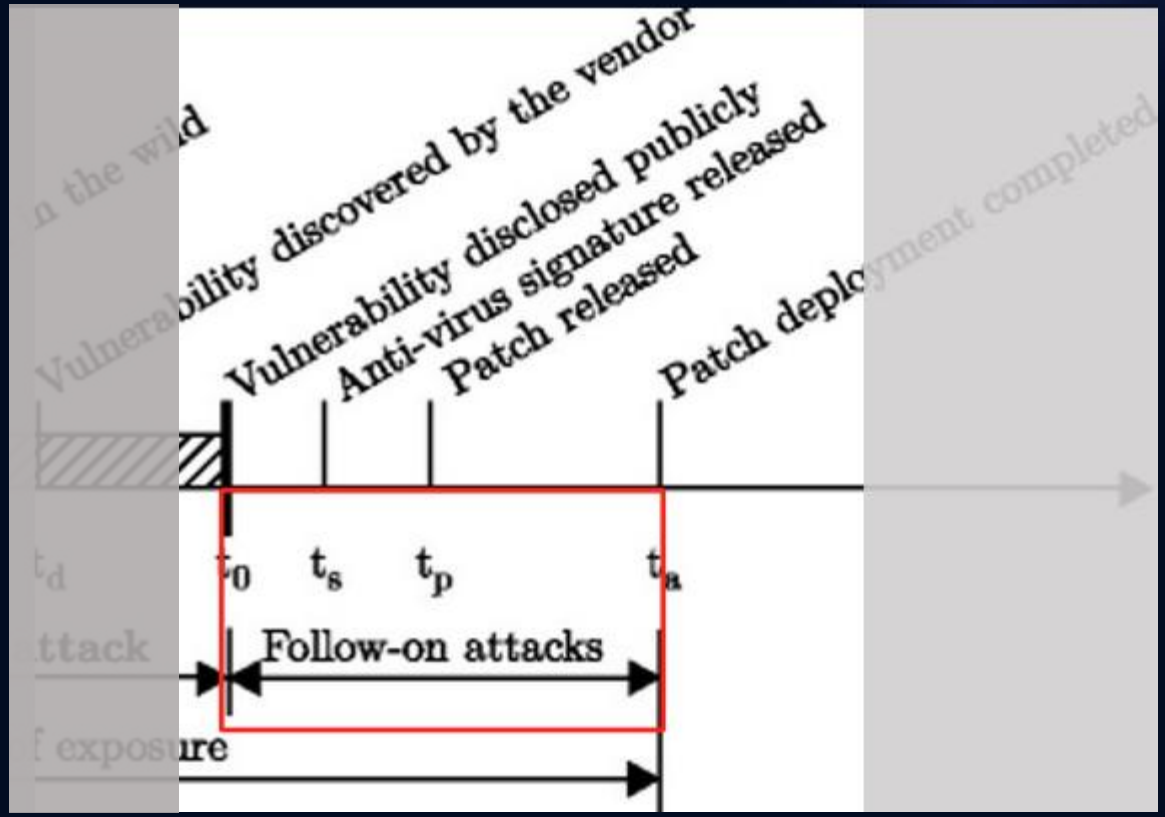
Vulnerability lifecycle pipeline

- According to the vulnerability lifecycle, it needs to deploy the patch for approaching the mitigation stage.
- In this period, it needs an auto patch update process or manual patch update to mitigate the vulnerability.



Vulnerability lifecycle pipeline

- It means that the environment is **exposed to the threats for a period**.
- Before approaching the mitigation stage, it needs a method or mechanism to decrease the risk of threats.



Automated extraction attack patterns

Automated extraction of attack vector

- Use AI LLM to analysis the vulnerability report and extract the attack patterns and vectors.
- After extracting the attack patterns and vectors, enhancing the knowledgebase of LLM model will avoid the hallucination.

Automated extraction of attack vector

CVE-2012-6439 Detail

MODIFIED

This CVE record has been updated after NVD enrichment efforts were completed. Enrichment data supplied by the NVD may require amendment due to these changes.

Description

Rockwell Automation EtherNet/IP products; 1756-ENBT, modules; CompactLogix L32E and L35E controllers; 1788 adapter; ControlLogix 18 and earlier; CompactLogix 18 a CompactLogix controllers 19 and earlier; SoftLogix contr GuardLogix controllers 20 and earlier; and MicroLogix 11 (control and communication outage) via a CIP message

Vulnerability Characterization

Vulnerability Overview

Improper Access Control—Change IP

When an affected product receives a valid CIP message from an unauthorized or unintended source to Port 2222/TCP, Port 2222/UDP, Port 44818/TCP, or Port 44818/UDP that changes the product's configuration and network parameters, a DoS condition can occur. This situation could cause loss of availability and a disruption of communication with other connected devices.

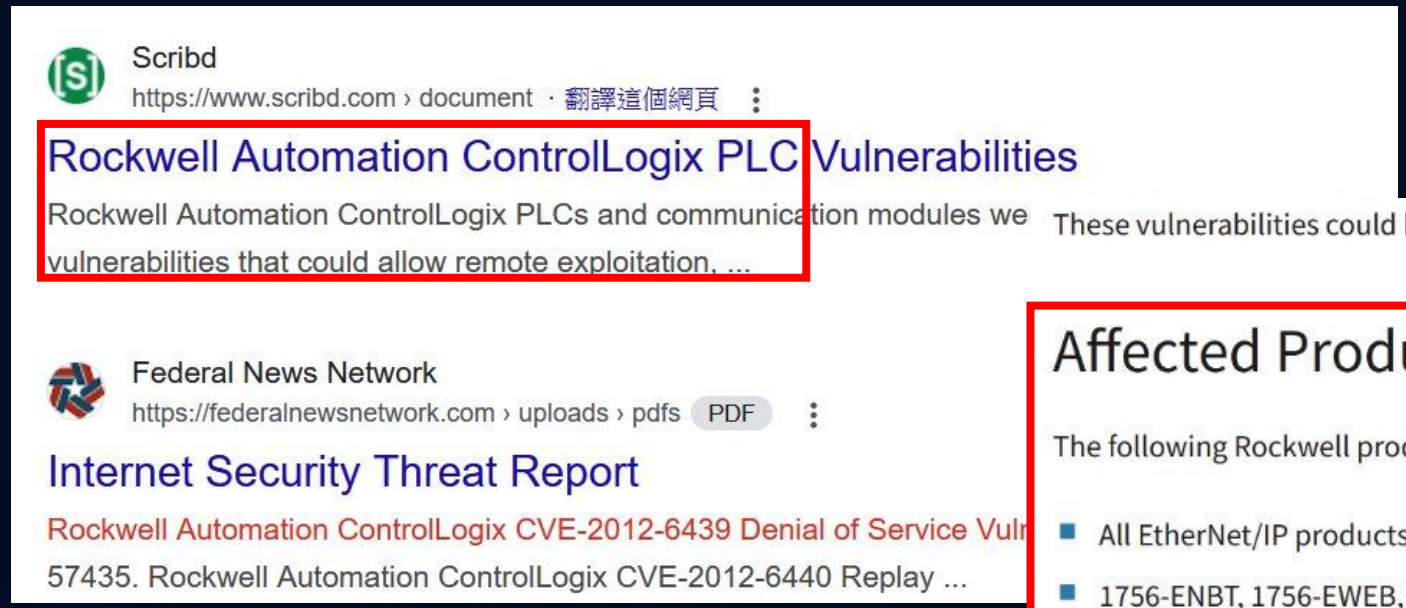
CVE-2012-6439 has been assigned to this vulnerability. A CVSS v2 base score of 8.5 has been assigned; the CVSS vector string is (AV:N/AC:L/Au:N/C:N/I:P/A:C).

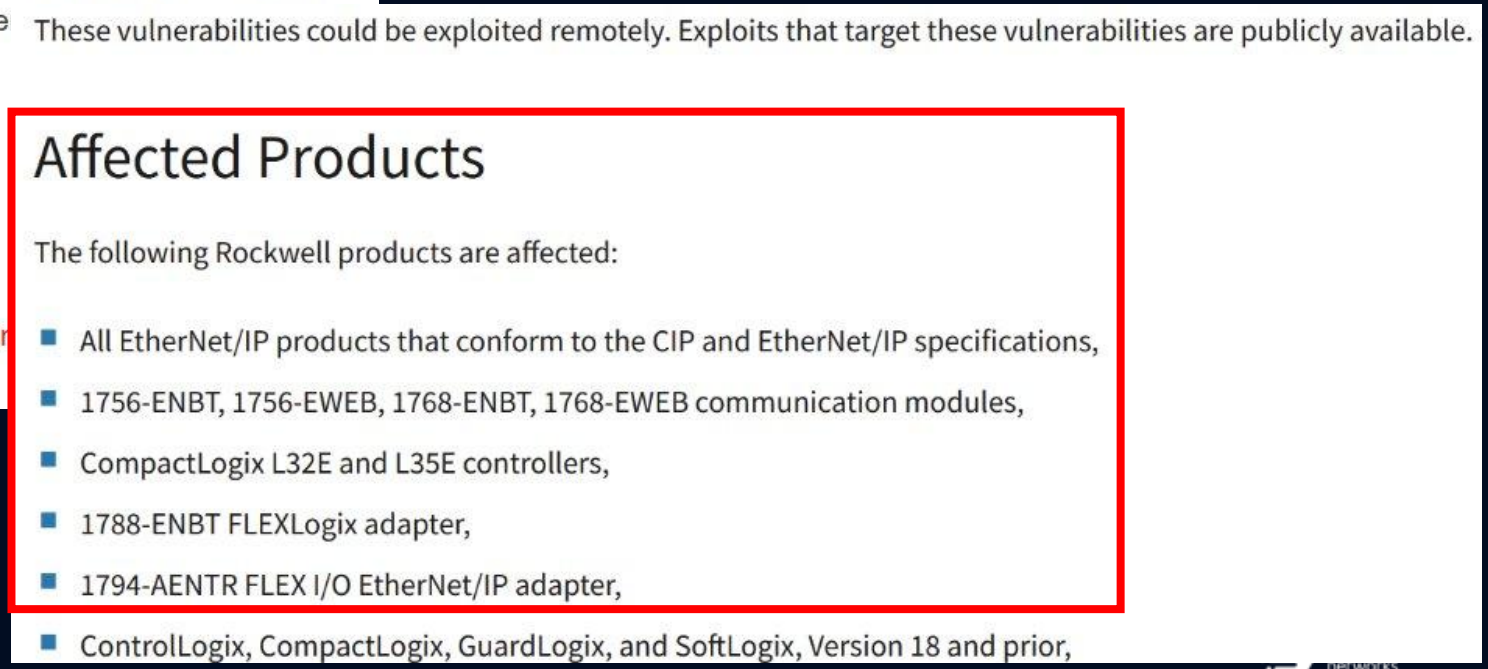
Automated extraction of attack vector

- Under the extraction process, it also can use text analysis and semantic parsing to let LLM to understand **complex relationship of attack vectors**.
- Similarly, the result also can optimize the knowledgebase and prompt of extraction process.

Automated extraction of attack vector

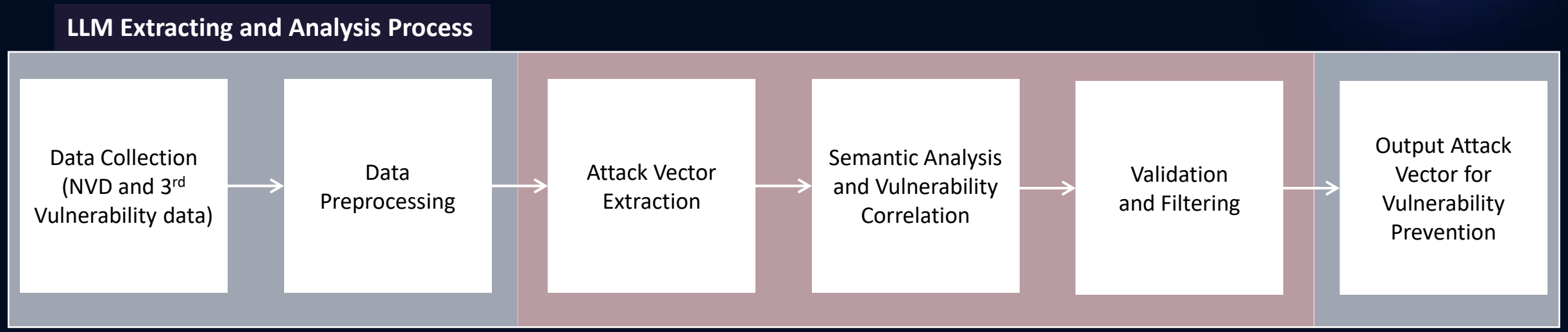
- For example, input the 3rd-party vulnerability and threat report to identify attack detail to extract the relationship of affected vendor, production and vulnerability.





Vulnerability prevention flowchart

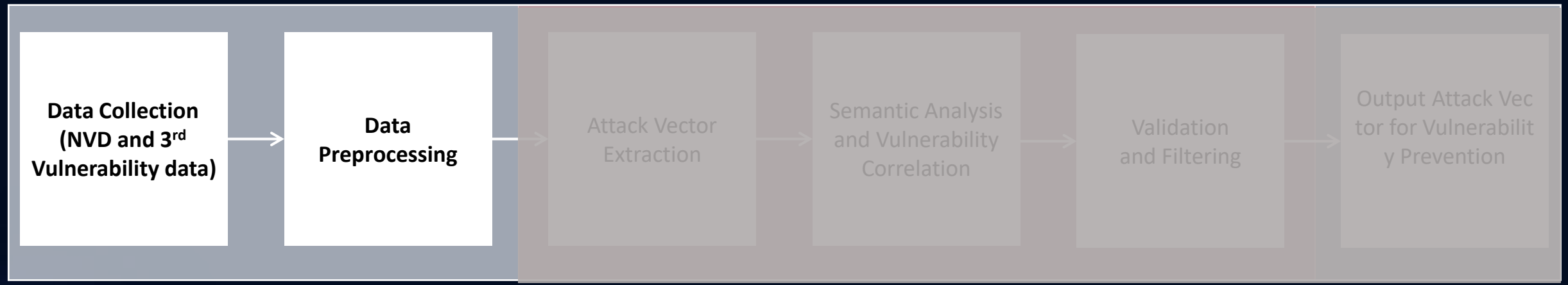
Vulnerability prevention flowchart



Vulnerability prevention flowchart

- **Data collection and preprocessing**

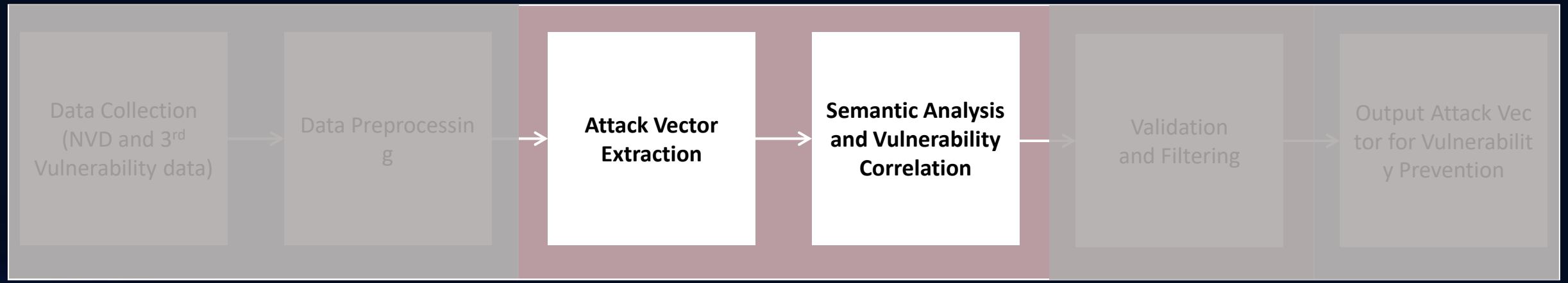
  Collect raw data from multiple sources for preprocessing to the same format



Vulnerability prevention flowchart

- **Attack vector extraction and analysis**

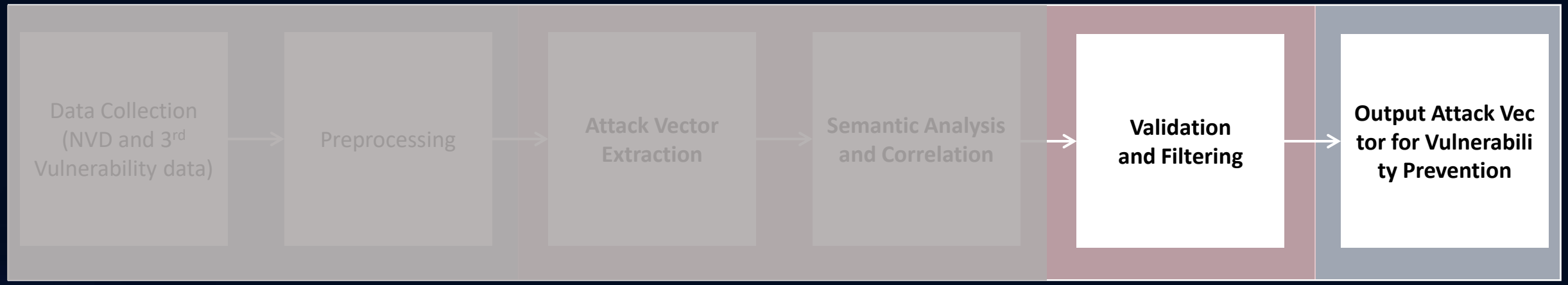
  To extract the specific attack vector and pattern from raw data and build the knowledgebase to enhance the accuracy of AI result.



Vulnerability prevention flowchart

- **Validation and filtering and output**

  Prepare the test set to validate and filter the AI result. According to the result, we optimize the knowledgebase and attack vector extraction process.



Benefits of vulnerability prevention

Benefits of vulnerability prevention

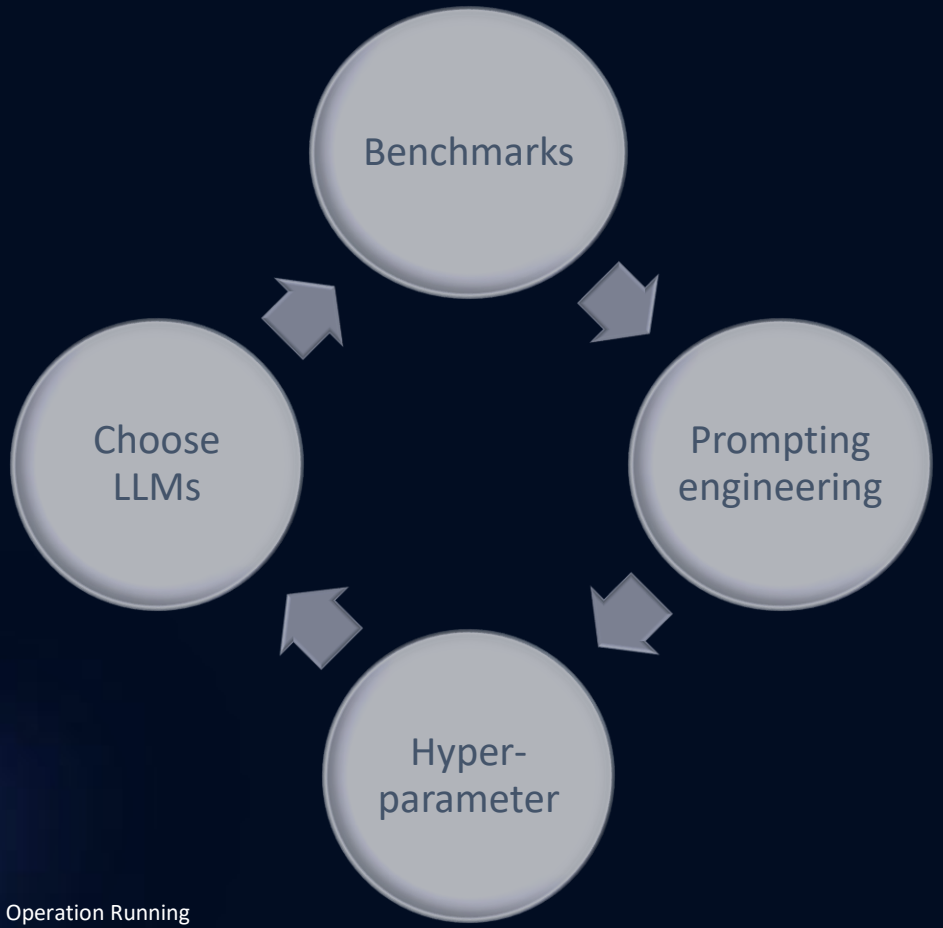
- In real-world scenarios, patch of vulnerability often deployed too late to achieve vulnerability mitigation, already impacting customers' environments.
- A vulnerability prevention mechanism can alert customers in the early stage of vulnerability lifecycle, providing timely intervention opportunities.
- By focusing on affected protocols and CVSS, customers can pinpoint critical weaknesses and prioritize appropriate actions for resolution.

Vulnerability prevention demonstration

Optimization Process

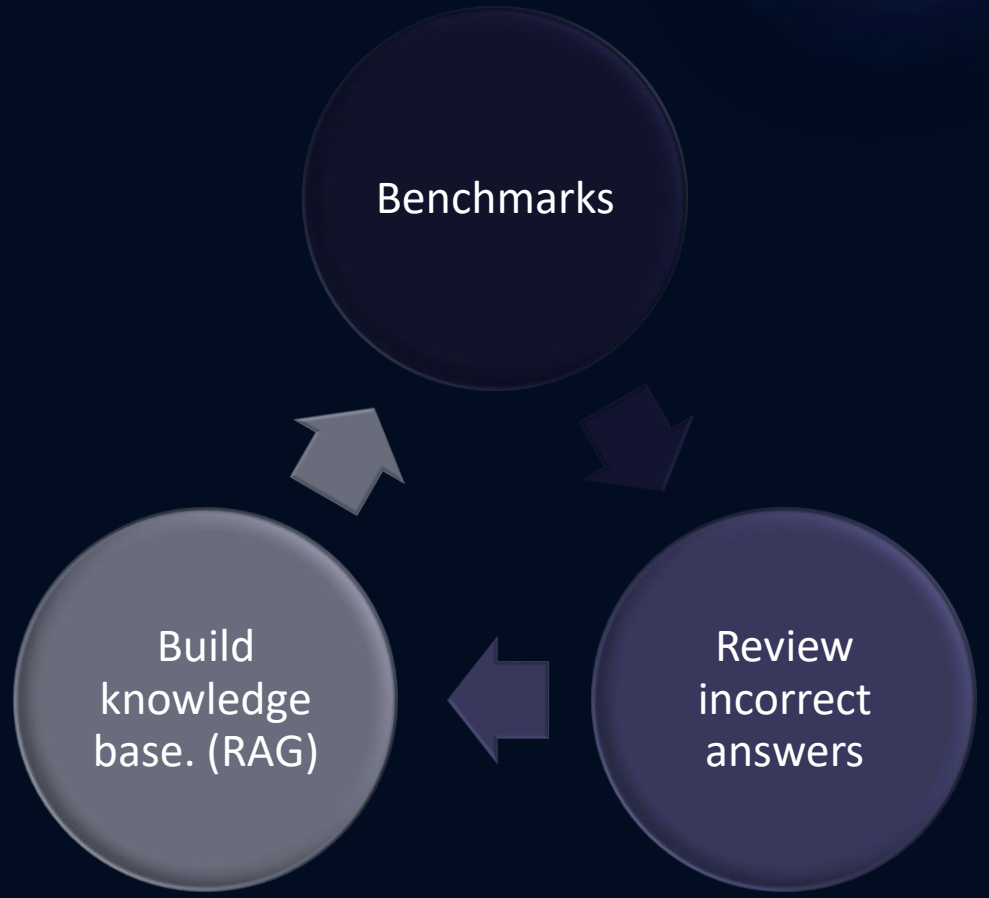
Basic Courses

Understanding the question



Professional Courses

Answering the question



Optimization Process

Basic Courses

Understanding the question

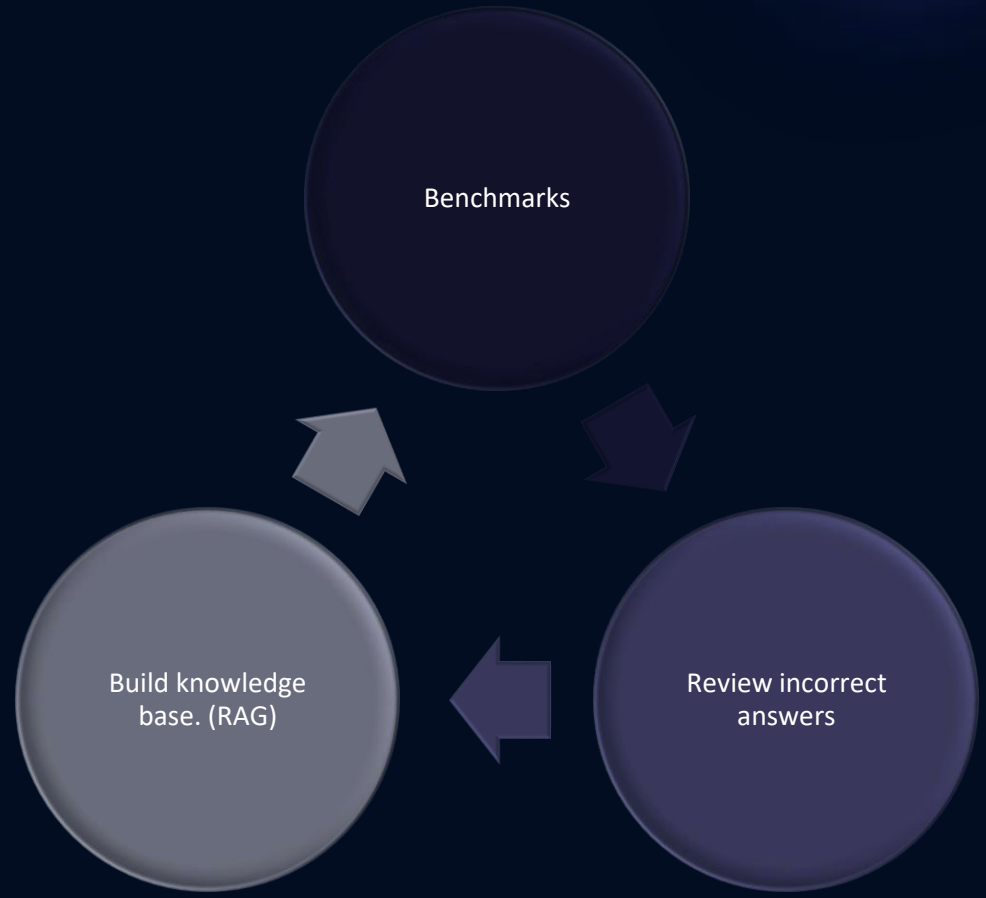
Benchmarks

You are an cybersecurity expert.
Based on the description, please determine if XXX and YYY, highlight the answer.
If you are not sure, just say unknown.
Response format: <Answer 1> ,<Answer 2>
And provide reason.

Hyper-parameter

Professional Courses

Answering the question



CVE-2012-6441

- Question: <CVE Description> and this vulnerability affected on: <CPE:Vendor> <CPE:Product>
  - Rockwell Automation EtherNet/IP products; 1756-ENBT, 1756-EWEB, 1768-ENBT, and 1768-EWEB communication modules; CompactLogix L32E and L35E controllers; 1788-ENBT FLEXLogix adapter; 1794-AENTR FLEX I/O EtherNet/IP adapter; ControlLogix 18 and earlier; CompactLogix 18 and earlier; GuardLogix 18 and earlier; SoftLogix 18 and earlier; CompactLogix controllers 19 and earlier; SoftLogix controllers 19 and earlier; ControlLogix controllers 20 and earlier; GuardLogix controllers 20 and earlier; and MicroLogix 1100 and 1400 allow remote attackers to obtain sensitive information via a crafted CIP packet. and this vulnerability affected on: rockwellautomation guardlogix_controllers
- Answer:
  - Server
  - CIP

Server, CIP

The description mentions "remote attackers" obtaining sensitive information through "crafted CIP packets". This indicates the vulnerability lies within the server-side implementation of the Common Industrial Protocol (CIP) used for industrial automation communication. CIP is a Layer 7 protocol operating above TCP/IP.

CVE-2010-2861

- Quesetion: <CVE Description> and this vulnerability affected on: <CPE:Vendor> <CPE:Product>
  - Multiple directory traversal vulnerabilities in the administrator console in Adobe ColdFusion 9.0.1 and earlier allow remote attackers to read arbitrary files via the locale parameter to (1) CFIDE/administrator/settings/mappings.cfm, (2) logging/settings.cfm, (3) datasources/index.cfm, (4) j2eepackaging/editarchive.cfm, and (5) enter.cfm in CFIDE/administrator/. and this vulnerability affected on: adobe coldfusion
- Answer:
  - Server
  - HTTP

Server, HTTP

Reason: The vulnerability description mentions "administrator console" and file paths like "CFIDE/administrator/settings/mappings.cfm", indicating a web-based server-side application. These are typically accessed using the HTTP protocol, which operates at Layer 7 of the OSI model.

CVE-2015-0984 – Incorrect results

- Question:
  - Directory traversal vulnerability in the FTP server on Honeywell Excel Web XL1000C50 52 I/O, XL 1000C100 104 I/O, XL1000C500 300 I/O, XL1000C1000 600 I/O, XL1000C50U 52 I/O UUKL, XL10 00C100U 104 I/O UUKL, XL1000C500U 300 I/O UUKL, and XL1000C1000U 600 I/O UUKL controll ers before 2.04.01 allows remote attackers to read files under the web root, and consequently o btain administrative login access, via a crafted pathname. and this vulnerability affected on: hon eywell excel_web_xl_1000c1000_600_i/o
- Answer:
  - Server
  - Unknown

Server,
This vulnerability occurs in the **FTP server** . The description explicitly states "directory traversal vulnerability in the FTP server".

Add Protocol information to knowledgebase

Well-known ports [edit]

This is a dynamic list and may never be able to satisfy particular standards for completeness. You can help by adding missi items with reliable sources.

The port numbers in the range from 0 to 1023 (0 to $2^{10} - 1$) are the *well-known ports* or *system ports*.[3] They are used by syste processes that provide widely used types of network services. On Unix-like operating systems, a process must execute with superuser privileges to be able to bind a network socket to an IP address using one of the well-known ports.[5]

Well-known ports [hide]

Port	TCP	UDP	SCTP	DCCP	Description
0	Reserved				In programming APIs (not in communication between hosts), requests system-allocated (dynamic) port[6]
1	Yes	Assigned			TCP Port Service Multiplexer (TCPMUX). Historic. Both TCP and UDF have been assigned to TCPMUX by IANA,[2] but by design only TCP i specified.[7]
2	Assigned				compressnet (Management Utility)[3]
3	Assigned				compressnet (Compression Process)[3]
5	Assigned				Remote Job Entry[8] was historically using socket 5 in its old socket fo while MIB PIM has identified it as TCP/5[9] and IANA has assigned bo TCP and UDP 5 to it.
7	Yes				Echo Protocol[10][11]
9	Yes		Yes[12]	Assigned	Discard Protocol[13]
	No	Unofficial			Wake-on-LAN[14]
11	Yes				Active Users (systat service)[15][16]
13	Yes				Daytime Protocol[17]

Protocols [edit]

The IETF definition document for the application layer in the Internet Protocol Suite is RFC 1123. It provided an initial set of protocols that covered the major aspects of the functionality of the early Internet:[6]

- Hypertext documents: Hypertext Transfer Protocol (HTTP)
- Remote login to hosts: Telnet, Secure Shell
- File transfer: File Transfer Protocol (FTP), Trivial File Transfer Protocol (TFTP)
- Electronic mail transport: Simple Mail Transfer Protocol (SMTP)
- Networking support: Domain Name System (DNS)
- Host initialization: BOOTP
- Remote host management: Simple Network Management Protocol (SNMP), Common Management Information Protocol over TCP (CMOT)

Examples [edit]

Additional notable application-layer protocols include the following:

- 9P, Plan 9 from Bell Labs distributed file system protocol
- AFP, Apple Filing Protocol
- APPC, Advanced Program-to-Program Communication
- AMQP, Advanced Message Queuing Protocol
- Atom Publishing Protocol
- BEEP, Block Extensible Exchange Protocol
- Bitcoin
- BitTorrent
- CFDP, Coherent File Distribution Protocol
- CoAP, Constrained Application Protocol
- DDS, Data Distribution Service
- NNTP, Network News Transfer Protocol
- NTCIP, National Transportation Communications for Intelligent Transportation System Protocol
- NTP, Network Time Protocol
- OSCAR, AOL Instant Messenger Protocol
- POP, Post Office Protocol
- PNRP, Peer Name Resolution Protocol
- RDP, Remote Desktop Protocol
- RELP, Reliable Event Logging Protocol
- RFB, Remote Framebuffer Protocol
- Rlogin, Remote Login in UNIX Systems

CVE-2015-0984 – Fix by RAG

- Question:
  - Directory traversal vulnerability in the FTP server on Honeywell Excel Web XL1000C50 52 I/O, XL 1000C100 104 I/O, XL1000C500 300 I/O, XL1000C1000 600 I/O, XL1000C50U 52 I/O UUKL, XL10 00C100U 104 I/O UUKL, XL1000C500U 300 I/O UUKL, and XL1000C1000U 600 I/O UUKL controll ers before 2.04.01 allows remote attackers to read files under the web root, and consequently o btain administrative login access, via a crafted pathname. and this vulnerability affected on: hon eywell excel_web_xl_1000c1000_600_i/o
- Answer:
  - Server
  - FTP ~~Unknown~~

Server, FTP

The vulnerability is described as affecting the FTP server on Honeywell Excel Web controllers, indicating a flaw within the server's service, not the client application. Furthermore, directory traversal exploits often target file systems accessible via network protocols like FTP.

CVE-2024-32845 – Incorrect results

- Question:
  - An unspecified SQL injection in Ivanti EPM before 2022 SU6, or the 2024 September update allows a remote authenticated attacker with admin privileges to achieve remote code execution.
    and this vulnerability affected on: ivanti endpoint_manager
- Answer:
  - Server
  - SQL

Server, SQL

Reasoning: The description explicitly states "unspecified SQL injection," indicating the vulnerability lies within the server-side database handling of Ivanti EPM. SQL injection attacks target database systems, which are typically part of a server's infrastructure.

CVE-2024-32845 – Fix by RAG

- Question:
  - An unspecified SQL injection in Ivanti EPM before 2022 SU6, or the 2024 September update allows a remote authenticated attacker with admin privileges to achieve remote code execution.
    and this vulnerability affected on: ivanti endpoint_manager
- Answer:
  - Server
  - HTTP ~~SQL~~

Expert rules.md

```
** Command injection usually use HTTP Protocol
** SQL injection usually use HTTP Protocol
```

Server, **HTTP**

Reasoning: SQL injection vulnerabilities typically reside on the server-side as they exploit weaknesses in how a server processes database queries. Since Ivanti Endpoint Manager is a server-based product, and the vulnerability description mentions remote code execution (a common consequence of server-side SQL injection), it's highly probable that the vulnerability affects the server component.
Furthermore, most management consoles and tools like Ivanti Endpoint Manager utilize **HTTP** for communication between clients and the server.

CVE-2022-25767 – Fix by RAG

- Question:
  - All versions of package com.bstek.ureport:ureport2-console are vulnerable to Remote Code Execution by connecting to a malicious database server, causing arbitrary file read and deserialization of local gadgets. and this vulnerability affected on: ureport2_project ureport2
- Answer:
  - Client ~~Server~~
  - HTTP

Expert rules.md

```
### Client-Side Vulnerability Characteristics
**General Characteristics**:
1. Mention of terms:
   - "Opening malicious files" is Client-Side.
   - "Interacting with malicious web servers" is Client-Side.
   - "Connecting to a malicious server" is Client-Side.
   - "Connecting to a malicious database" is Client-Side.
   - "Vulnerabilities in browsers" is Client-Side.
   - "Vulnerabilities in desktop applications" is Client-Side.
```

Results

Question	RAG	Llama3.1-8B	Gemma2-9B	Gemma2-27B
Target protocol of the vulnerability	N/A	60%	82%	86%
	Common Protocol List + Expert rules	87%	90%	91%

4000 Question Runtime < 60 Minutes

Question	RAG	Llama3.1-8B	Gemma2-9B	Gemma2-27B
Target role (Client | Server) of the vulnerability	N/A	55%	82%	77%
	Expert rules	74%	85%	90%

Hardware/Software Resources

Hardware	Details
CPU	AMD R7-9700X
GPU	NVIDIA RTX4090 24GB
RAM	DDR5 48GB *2
HDD	PCIE 4.0 SSD 2TB
PSU	1300W (80 PLUS GOLD)

Software	Details
Proxmox VE	8.2.7
Docker	27.3.1
Ollama	0.4.0
LM	Gemma2-27B

Knowledge Base	Rules
Common Protocol List	72
Expert Rules	41


txOne
networks