Capstone Synopsis - PGPCS June 2023

<Rajan Kumar Sahu>

*Synopsis, preferably, should be of about 2-3 pages. The content should be as brief as is sufficient enough to explain the objective and implementation of the project that the Learner is going to take up. The write up must adhere to the guidelines and should include the following.*

# Name / Capstone Final Report:

The Wazuh project is an open-source security platform that provides real-time threat detection, incident response, and compliance management capabilities. It aims to help organizations enhance their security posture by monitoring and analyzing security events across their IT infrastructure.

*.*

# Objective / Problem Statement:

Wazuh Agent: The Wazuh agent is a lightweight software installed on the monitored endpoints, such as servers, workstations, or cloud instances. It collects and analyzes security-related data from various sources on the endpoint, including log files, system events, file integrity changes, and more. The agent normalizes and sends this data to the central server for further analysis.

Wazuh Server: The Wazuh server receives and processes the data sent by the agents. It performs real-time log analysis, threat detection, and correlation using an extensive set of predefined security rules. These rules cover a wide range of security scenarios, including intrusion detection, malware detection, file integrity monitoring, and compliance checks. When a potential security incident is detected, the server can generate alerts or trigger automated responses.

Wazuh Management Console: The Wazuh management console provides a user-friendly interface for managing and monitoring the Wazuh infrastructure. It allows security administrators to configure the server and agents, create custom security rules, view and investigate security events, and generate reports. The management console also provides integration with other security tools and platforms, enhancing the overall security ecosystem.

Vulnerability management with the help of wazuh: Wazuh vulnerability management by integrating with vulnerability scanning tools and providing real-time monitoring and alerting capabilities. Here's how you can use Wazuh for vulnerability management:

# Proposed Solution:

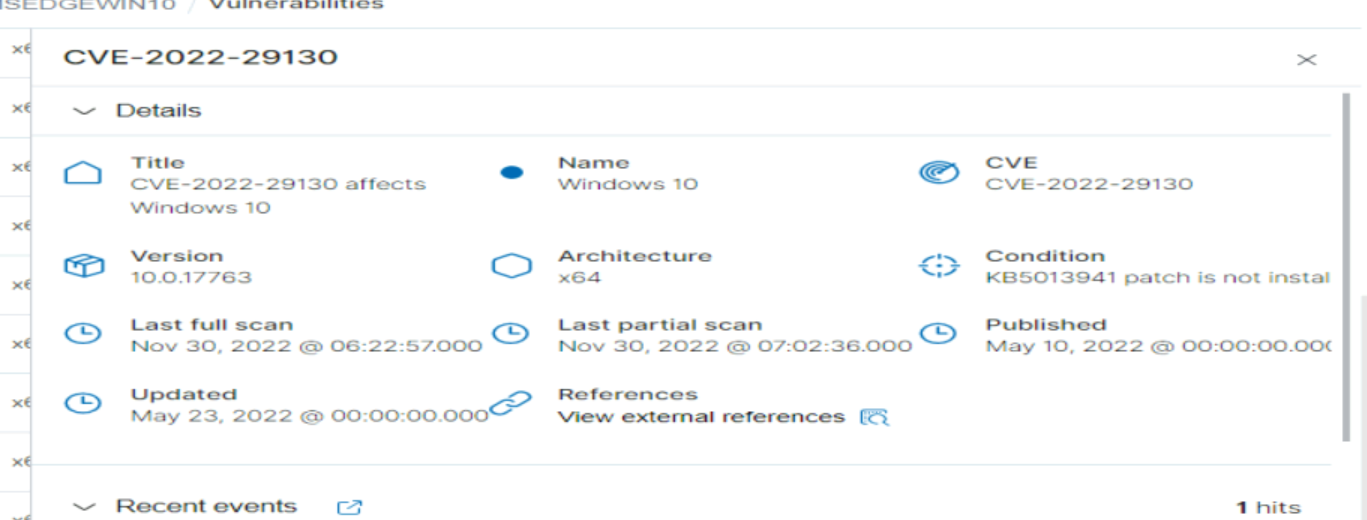
1. Configure vulnerability detection rules: Wazuh provides a set of pre-configured rules specifically designed to detect vulnerabilities. These rules analyze log data, system configurations, and network traffic to identify potential security weaknesses. You can fine-tune these rules based on your specific needs and risk tolerance.
2. Enable vulnerability monitoring: By enabling vulnerability monitoring in Wazuh, the system will continuously analyze events and log data for signs of vulnerabilities. Wazuh can detect indicators such as outdated software versions, missing security patches, misconfigurations, weak passwords, and other common vulnerability indicators.
3. Generate vulnerability reports: Wazuh provides reporting capabilities that allow you to generate vulnerability reports based on the detected issues. These reports can provide an overview of the vulnerabilities found, their severity, affected systems, and recommended remediation steps. The reports can be scheduled to run periodically or generated on-demand as needed.
4. Generate reports: Once the visualizations and dashboards are created in Kibana, you can generate reports based on them. Kibana provides options to export reports in various formats such as PDF, CSV, or PNG. You can schedule the reports to run periodically or generate them on-demand as needed.

* **Configure vulnerability data collection**
* **Set up Elasticsearch indices**
* **Define report requirements**
* **Utilize Kibana reporting features**

TOP 4 CRITICAL VULNERABILITIES:

1: WINDOWS LDAP REMOTE CODE EXECUTION VULNERABILITY

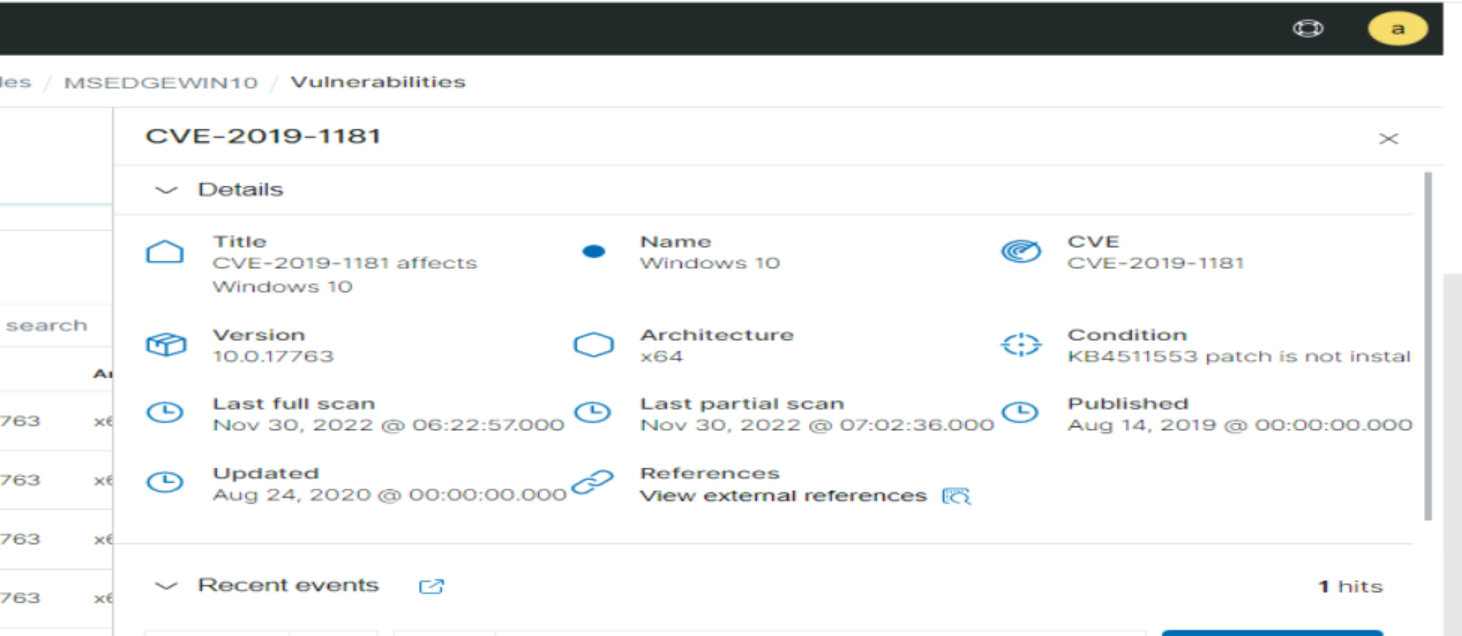
SOLUTION : MAY 10 ,2022 PATCH OR MORE RECENT PATCH KB5013941 NEED TO BE INSTALLED



2 CVE-2019-1181

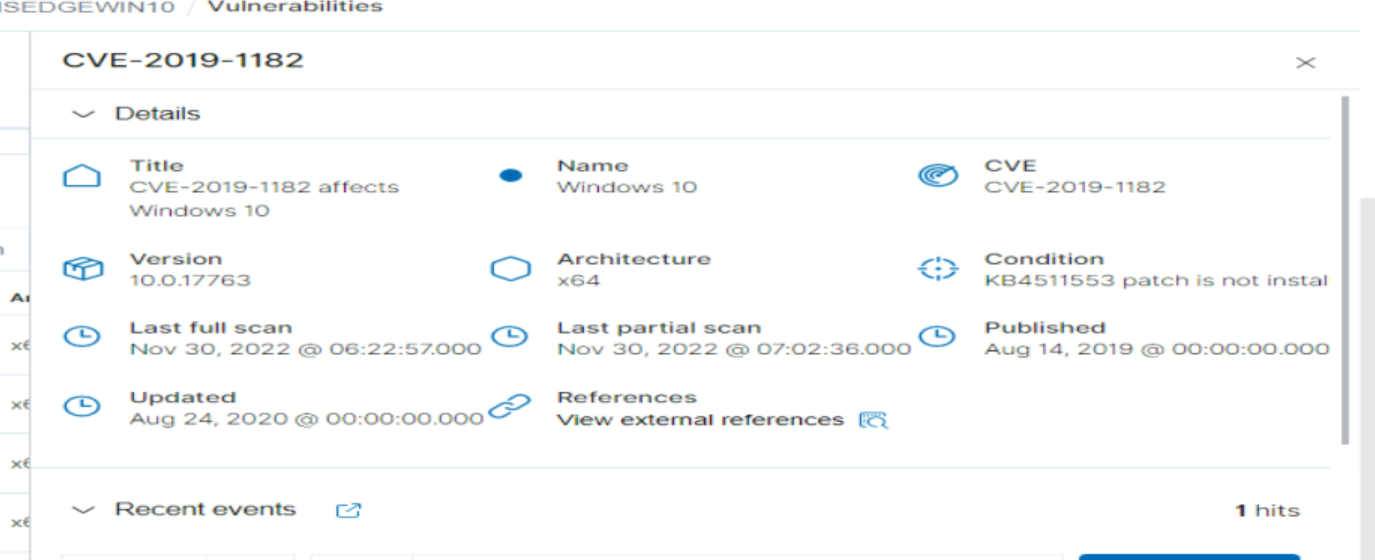
IMPROPER NEUTRALIZATION OF INPUT DURING WEB PAGE GENERATION (CROSS SITE SCRIPTING)

SOLUTION : NEED TO BE PATCHED TO (KB4511553) 6.1.0 VERSION



3. VISUAL SLIDE BOX VULNERABLE TO SQL INJECTION

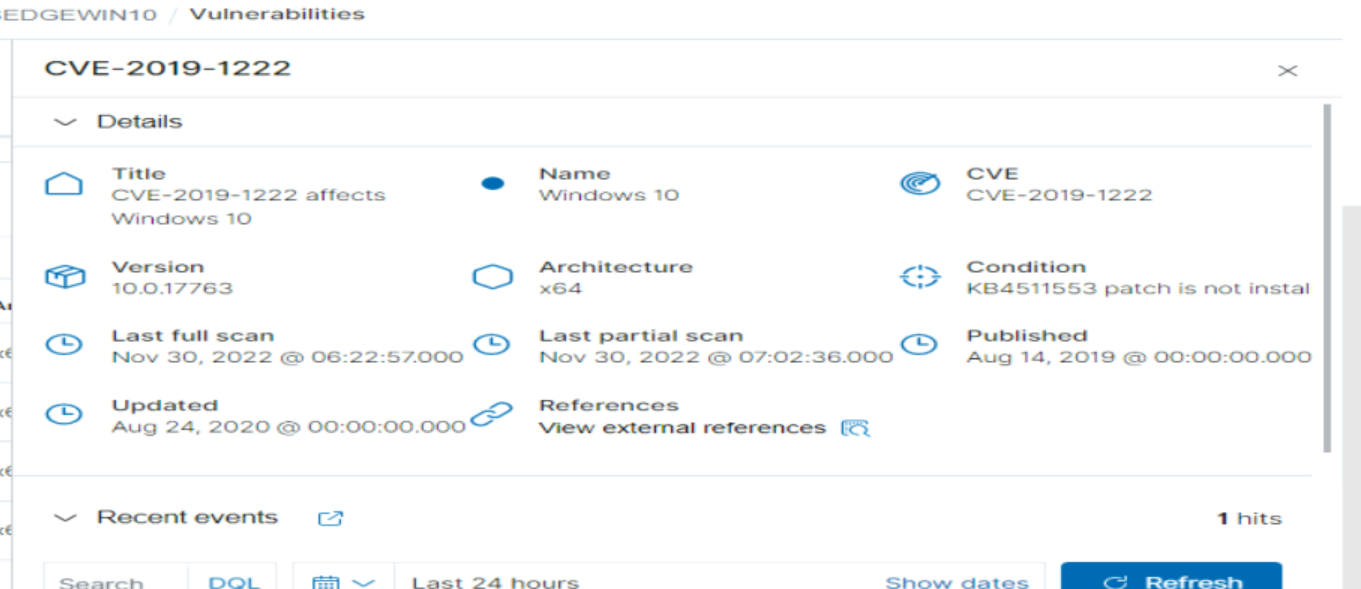
SOLUTION : UPDATE VISUAL SLIDE BOX BUILDER PROJECT TO ABOVE 3.2.9 VERSION



4. REMOTE CODE EXECUTION CODE VULNERABILITY EXITS IN REMOTE DESKTOP SERVICES

WORKAROUND : ENABLE NETWORK LEVEL AUTHENTICATION

BLOCK TCP PORT 3389 AT THE ENTERPRISE PERIMETER FIREWALL



Conclusion:

*The synopsis should conclude with identifying the following points:*

1. ***Real world impact*** *- Wazuh is a Very widely used open-source security platform that brings several real-world impacts and benefits to organizations.*

*Enhanced Security Monitoring: Wazuh provides organizations with robust security monitoring capabilities. By collecting and analyzing security event data from various sources such as logs, network traffic, and endpoints, Wazuh helps detect and respond to security incidents in real-time*

*Centralized Log Management: Wazuh acts as a centralized log management solution, allowing organizations to aggregate and store log data from different systems and applications. This centralized approach simplifies log analysis, correlation, and compliance reporting.*

*Threat Detection and Incident Response: Wazuh employs a range of detection techniques, including signature-based rules, anomaly detection, and integration with threat intelligence feeds. These capabilities enable Wazuh to identify and alert on a wide array of security threats, such as malware infections, unauthorized access attempts, configuration changes,*

*Compliance and Regulatory Requirements: Wazuh assists organizations in meeting compliance and regulatory requirements. It offers pre-configured security rulesets and compliance templates for frameworks like PCI DSS, GDPR, CIS benchmarks, and others. Wazuh helps automate compliance monitoring, generates reports,*

*Overall, Wazuh brings real-world impact by bolstering an organization's security posture, improving incident detection and response, simplifying compliance management, and promoting collaboration within the security community. These benefits contribute to a more resilient and secure environment, helping organizations protect their valuable assets, data, and reputation.*

1. **Any innovation:** Wazuh implemented several innovative approaches to improve the security of its systems.

* ***Agentless Based monitoring****: Wazuh can monitor systems without the need to install an agent on each host. This makes it easier to deploy and manage Wazuh, and it also reduces the attack surface of the systems being monitored.*
* ***Active response:*** *Wazuh can take active steps to respond to security incidents. This includes things like blocking malicious traffic, quarantining infected hosts, and resetting passwords.*
* ***Active response:*** *Wazuh can take active steps to respond to security incidents. This includes things like blocking malicious traffic, quarantining infected hosts, and resetting passwords.*
* ***Active response:*** *Wazuh can take active steps to respond to security incidents. This includes things like blocking malicious traffic, quarantining infected hosts, and resetting passwords.*

*Wazuh is a powerful and innovative security solution that can help organizations protect their systems from a wide range of threats.*

**Main achievements:**

* *Improved security: Wazuh has helped organizations improve their security by providing them with a powerful and innovative security solution. Wazuh has helped organizations detect and respond to threats more effectively, and it has also helped them to reduce the attack surface of their systems.*
* *Increased visibility: Wazuh has helped organizations increase their visibility into their security posture. Wazuh provides organizations with a centralized view of their security events, which makes it easier for them to identify and respond to threats.*
* *Reduced costs: Wazuh has helped organizations reduce their security costs. Wazuh is an open source solution, which means that it is free to use and modify. This has helped organizations to save money on their security budgets.*

**My learning goals from the Wazuh project:**

* Gain a deeper understanding of security threats and how to mitigate.
* How to use Wazuh to monitor and protect systems.
* Gain experience with open source software.
* different types of security threats that organizations face.
* Wazuh to collect and analyze security events.
* Wazuh to create rules and detections.
* Wazuh to integrate with other security systems.

I achieved these goals by participating in the Wazuh project and by working with other security professionals. I learned a lot about security threats and how to mitigate them. I also learned how to use Wazuh to monitor and protect systems.also gained experience with open source.

I am grateful for the opportunity to have participated in the Wazuh project. I learned a lot and I am confident that I can use my knowledge to help other organizations improve their security.