### **Nessus Plugins & Threat Detections And Response**

**Overview: -**

Nessus is a widely used vulnerability scanning tool that helps organizations identify and address security issues in their systems. It works by scanning networks, systems, and applications for vulnerabilities and providing detailed reports to assist in remediation efforts. Nessus uses plugins to perform various checks and tests for vulnerabilities.

**Nessus Plugins:**

1. **Vulnerability Detection:** Nessus plugins are responsible for detecting vulnerabilities in systems. These plugins are regularly updated to include new checks for the latest vulnerabilities and security issues. Each plugin corresponds to a specific type of vulnerability or security check.
2. **Compliance Checks:** Nessus plugins also include compliance checks to assess whether systems adhere to specific security policies, standards, or regulations. This helps organizations ensure that their systems meet the required security benchmarks.
3. **Configuration Auditing:** Nessus can audit system configurations to identify misconfigurations that may expose systems to security risks. This includes checks for insecure settings, open ports, and other configuration-related issues.
4. **Malware Detection**: Some plugins are designed to identify signs of malware or malicious activity on scanned systems. This includes looking for known malware signatures or indicators of compromise.
5. **Policy Auditing:** Nessus plugins can audit systems against predefined security policies to ensure that they align with the organization's security requirements.
6. **Web Application Scanning:** Nessus has plugins specifically designed for scanning and identifying vulnerabilities in web applications. This includes issues such as SQL injection, cross-site scripting (XSS), and other web-related vulnerabilities.

**Threat Detections and Response:**

While Nessus primarily focuses on vulnerability scanning, threat detection and response are broader concepts that involve monitoring for signs of malicious activity and responding to security incidents. Here's how these concepts relate to Nessus:

1. **Integration with SIEM (Security Information and Event Management**): Nessus scan results can be integrated with SIEM solutions to enhance threat detection capabilities. SIEM systems collect and analyze log data from various sources, helping to identify patterns of suspicious or malicious activity.
2. **Incident Response:** When Nessus identifies vulnerabilities or potential security issues, organizations can use this information as part of their incident response process. Remediation actions can be taken to address identified vulnerabilities and mitigate potential risks.
3. **Continuous Monitoring:** Nessus is often used as part of a continuous monitoring strategy, providing regular scans to ensure that systems remain secure over time. This aligns with the continuous monitoring aspect of threat detection.
4. **Collaboration with Other Security Tools:** Organizations may use Nessus in conjunction with other security tools, such as intrusion detection systems (IDS) or endpoint detection and response (EDR) solutions, to enhance their overall threat detection and response capabilities.

In summary, Nessus plugins are primarily focused on vulnerability scanning, while threat detection and response involve a broader set of activities aimed at monitoring and responding to malicious activities. Organizations often use Nessus as part of a comprehensive cybersecurity strategy that includes both vulnerability management and broader threat detection and response capabilities.

**Target website: - https://about.gitlab.com/**

**Target IP address: - 172.64.153.92**

**List of vulnerability:**

|  |  |  |  |
| --- | --- | --- | --- |
| **S.no** | **Vulnerability name** | **Severity** | **Plugins** |
| 1 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | Medium | 187444 |
| 2 | Improper Authentication | Critical | 187475 |
| 3 | Insertion of Sensitive Information into Log File | Low | 187471 |
| 4 | Improper Encoding or Escaping of Output | High | 187465 |
| 5 | Incorrect Authorization | Low | 187449 |

**REPORT**

**Vulnerability Name: -** Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

**Severity: -** Medium

**Plugin: -** 187444

**Description: -** The version of GitLab installed on the remote host is affected by a vulnerability, as follows: - An issue has been discovered in GitLab affecting all versions starting with 13.3. GitLab was vulnerable to a stored XSS by using the design feature in issues. (CVE-2021-22238)

**Solution: -** Upgrade to GitLab version 14.0.9, 14.1.4, 14.2.2 or later.

**Business Impact**: - A Cross-Site Scripting (XSS) vulnerability in a business's web application can have severe consequences, impacting both the organization and its users. XSS allows attackers to inject malicious scripts into web pages viewed by other users. This can lead to unauthorized access to sensitive information, such as login credentials or personal data, potentially resulting in identity theft or financial losses for affected users. Moreover, the compromised web application may be used to distribute malware or launch further attacks on the organization's infrastructure. Beyond the immediate security risks, the business may suffer reputational damage, loss of customer trust, and legal repercussions. Timely identification and remediation of XSS vulnerabilities are crucial to mitigate these risks and uphold the integrity of the business and its online services.

**Vulnerability Name: -** Improper Authentication

**Severity: -** Critical

**Plugin: -** 187475

**Description: -** The version of GitLab installed on the remote host is affected by a vulnerability, as follows: - Missing sanitization of logged exception messages in all versions prior to 14.7.7, 14.8 prior to 14.8.5, and 14.9 prior to 14.9.2 of GitLab CE/EE causes potential sensitive values in invalid URLs to be logged (CVE-2022-1157)

**Solution: -** Upgrade to GitLab version 14.7.7, 14.8.5, 14.9.2 or later.

**Business Impact**: - Improper Authentication within a business's systems can have significant and far-reaching consequences. Authentication serves as the cornerstone of secure access control, ensuring that only authorized individuals can access sensitive resources. When authentication mechanisms are compromised, unauthorized users may gain access to confidential data, financial records, or proprietary information. This breach of confidentiality can lead to severe financial losses, reputational damage, and legal ramifications, especially if the compromised access results in data breaches or regulatory non-compliance. Additionally, improper authentication may enable malicious actors to impersonate legitimate users, causing disruption to operations, service interruptions, and erosion of customer trust. To mitigate these risks, businesses must implement robust authentication processes, regularly assess their security posture, and promptly address any vulnerabilities to safeguard both their internal assets and customer data.

**Vulnerability Name: -** Insertion of Sensitive Information into Log File

**Severity: -** Low

**Plugin: -** 187471

**Description: -** The version of GitLab installed on the remote host is affected by a vulnerability, as follows: - Missing sanitization of logged exception messages in all versions prior to 14.7.7, 14.8 prior to 14.8.5, and 14.9 prior to 14.9.2 of GitLab CE/EE causes potential sensitive values in invalid URLs to be logged (CVE-2022-1157)

**Solution: -** Upgrade to GitLab version 14.7.7, 14.8.5, 14.9.2 or later.

**Business Impact**: - The insertion of sensitive information into log files poses a critical threat to business security and integrity. Log files are essential for monitoring system activities, troubleshooting, and investigating security incidents. When sensitive information, such as usernames, passwords, or proprietary data, is inappropriately inserted into log files, it creates a significant risk of unauthorized access and exposure. Malicious actors may exploit this vulnerability to gain unauthorized access to sensitive systems, compromise user accounts, or launch targeted attacks. The business impact extends beyond immediate security concerns, encompassing potential legal and regulatory consequences, reputational damage, and financial losses. Detecting and preventing the insertion of sensitive information into log files is crucial to maintaining the confidentiality and integrity of critical business data, preserving customer trust, and avoiding the far-reaching repercussions associated with data breaches and privacy violations.

**Vulnerability Name: -** Improper Encoding or Escaping of Output

**Severity: -** High

**Plugin: -** 187465

**Description: -** The version of GitLab installed on the remote host is affected by a vulnerability, as follows: - Improper input validation in all versions of GitLab CE/EE using send mail to send emails allowed an attacker to steal environment variables via specially crafted email addresses. (CVE-2022-0741)

**Solution: -** Upgrade to GitLab version 14.6.5, 14.7.4, 14.8.2 or later.

**Business Impact**: - Improper encoding or escaping of output in a business's software applications can have profound implications for both the organization and its users. This vulnerability can be exploited by attackers to inject malicious code into the application's output, leading to a range of security issues such as Cross-Site Scripting (XSS) attacks. The business impact includes the potential compromise of sensitive user data, unauthorized access to accounts, and the manipulation of user interactions within the application. Beyond the immediate security concerns, there is a risk of reputational damage, erosion of customer trust, and legal consequences if customer information is compromised. Moreover, the organization may face operational disruptions, remediation costs, and increased efforts to address vulnerabilities and restore the integrity of its software. To mitigate these risks, businesses must prioritize secure coding practices, implement robust input validation mechanisms, and conduct regular security assessments to identify and rectify any instances of improper encoding or escaping in their applications.

**Vulnerability Name: -** Incorrect Authorization

**Severity: -** Low

**Plugin: -** 187449

**Description: -** The version of GitLab installed on the remote host is affected by a vulnerability, as follows: - Improper access control in the GitLab CE/EE API affecting all versions starting from 9.4 before 14.3.6, all versions starting from 14.4 before 14.4.4, all versions starting from 14.5 before 14.5.2, allows an author of a Merge Request to approve the Merge Request even after having their project access revoked (CVE-2021-39945)

**Solution: -** Upgrade to GitLab version 14.3.6, 14.4.4, 14.5.2 or later.

**Business Impact**: - Incorrect authorization within a business's systems can result in severe consequences, jeopardizing the confidentiality, integrity, and availability of sensitive resources. When users are granted improper or unauthorized access privileges, it opens the door to potential data breaches, unauthorized transactions, and malicious activities within the organization's digital environment. The impact extends to financial losses, as attackers may exploit these vulnerabilities for monetary gain or to disrupt critical business operations. Additionally, the compromised authorization can lead to regulatory non-compliance, exposing the business to legal consequences and reputational damage. Customers' trust may be eroded if their sensitive information is accessed without proper authorization. The organization may also face operational disruptions, remediation costs, and the need for extensive security measures to correct the misconfigured authorization settings. Proper access controls, regular reviews of permissions, and stringent authorization policies are crucial for businesses to mitigate the risks associated with incorrect authorization and ensure the overall security of their systems and sensitive data.

Prepared By: Sheeja Pon Chakravarthy, AP/CSE,

Coimbatore Institute of Technology.