

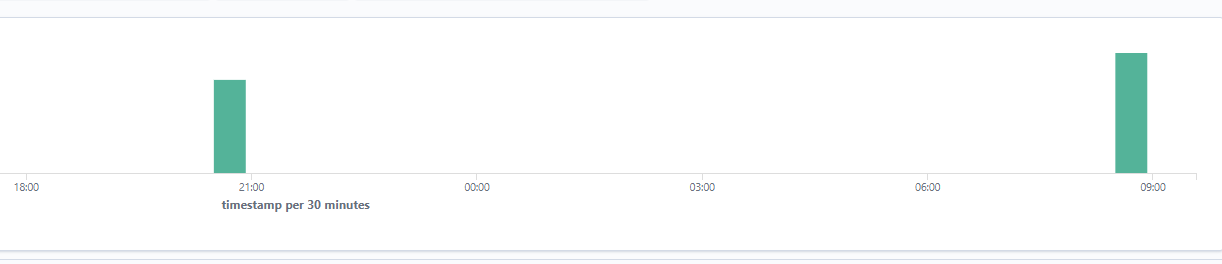
MITRE-2024-10-1`

**MITRE ATT&CK Report**

|  |  |
| --- | --- |
| **Agent ID**: 199, 203  **Agent IP Address:** 46.250.229.119, 10.0.10.154 | **Agent Name:** app1.msumedicalcentre.com, app2.msumedicalcentre.com, db3.msumedicalcentre.com, eklas.jgu.ac.id |
|  | **Group(s):** default, LinuxSVR |
| **Operating system**: Ubuntu 18.04.6 LTS, Windows Server | **Cluster node**: node01 |
| **Version:** v4.7.3, v4.9.0 | **Registration date**: 11th October 2024 @ 10:00:00.000 |
| **Status**: Active  **Legend:** | **PIC**: SHAHSWIENE |

|  |  |  |
| --- | --- | --- |
| No. | Color | Significance |
| 1 |  | Important Details |
| 2 |  | Critical Details |
| 3 |  | False Alerts |
| 4 |  | Compliance Standards |
| 5 |  | Attacker Sources |
| 6 |  | Affected Data URL/File |

**1. Registry Value Entry Deleted.**

****

**Figure 1: Registry Value Entry Deleted (timestamps v count rule fired).**

1. **Alert Description:**

* **Level**: 5 (Moderate Severity)
* **Description**: Registry Value Entry Deleted.
* **Groups**: ossec, syscheck, syscheck\_entry\_deleted, syscheck\_registry

**II. Rule Information:**

* **Rule ID**: 751
* **Mail Notification:** No
* **Compliance Standards:**
  + PCI DSS: 11.5
  + TSC: CC6.6, CC7.1, CC8.1, CC6.1, CC6.8, CC7.2, CC7
  + NIST 800-53: SI.4.7
  + GDPR: II\_5.1.f

**III. Alert Details:**

* **Location**: /var/log/nginx/cms-msu\_access.log, /var/log/nginx/msu\_access.log
* **Decoder**: web-accesslog
* **Agent** **Information**:
  + **IP**: 10.0.16.52, 10.0.16.53, 10.0.16.47
  + **Name**: app1.msumedicalcentre.com, app2.msumedicalcentre.com, db3.msumedicalcentre.com
  + **ID:** 009, 010, 008
* **Full Log:**

app1.msumedicalcentre.com:

* + Registry Value '[x32] HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\ASP.NET\_4.0.30319\Names\GRRhgoolBZGFss5VLo7HnRYCFdtY2hBldByKGYFA5cGqqtrpWiclAtJGOjHB8Uy4SY07wrmB3zb5mn4NHV28d2yxNGTcojOVbug0Ll4NCNCr8aAtvQjwyH' deleted Mode: scheduled

app2.msumedicalcentre.com:

* + Registry Value '[x32] HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\ASP.NET\_4.0.30319\Names\mJlfutS14lbSAyx3akJJnm0TcDkx00m6g56ld2sB4zz4Icvu8m95ZDH2oCS2lDrlrwrToEzNLje8vGyEW6ihNnWxHFxN3TUMlNVADmMsDM5Ig8IHXZW8Oi' deleted Mode: scheduled
  + Registry Value '[x32] HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\MpKsl6b299212\Version' deleted Mode: scheduled
  + Registry Value '[x32] HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\MpKsl6b299212\ImagePath' deleted Mode: scheduled
  + Registry Value '[x32] HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\MpKsl6b299212\ErrorControl' deleted Mode: scheduled
  + Registry Value '[x32] HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\MpKsl6b299212\DeviceName' deleted Mode: scheduled
  + Registry Value '[x32] HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\MpKsl6b299212\AllowedProcessName' deleted Mode: scheduled

db3.msumedicalcentre.com:

* + Registry Value '[x32] HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\MpKsl4dc81977\Version' deleted Mode: scheduled
  + Registry Value '[x32] HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\MpKsl4dc81977\ImagePath' deleted Mode: scheduled
  + Registry Value '[x32] HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\MpKsl4dc81977\ErrorControl' deleted Mode: scheduled
  + Registry Value '[x32] HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\MpKsl4dc81977\DeviceName' deleted Mode: scheduled
  + Registry Value '[x32] HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\MpKsl4dc81977\AllowedProcessName' deleted Mode: scheduled
* **System Check Path**: HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\MpKsl4dc81977
* **Ticket ID**: NA

**IV. Significant Findings and Impact:**

* **Event** **Type**: Defence Evasion
* **Observation**: There are several services modification was occurred in HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\MpKsl4dc81977 path
* **Impact**: .

### **V. Remediation Measures:**

1. **Immediate Investigation:**
   * Conduct a thorough investigation to determine the cause of the registry deletions. Assess whether these changes were authorized or if they indicate malicious activity.
   * Review logs from the affected systems to identify any suspicious activity leading up to the registry changes.
2. **Restore Deleted Registry Values:**
   * If it’s determined that the deletions were unauthorized, restore the deleted registry values from backup if available.
   * Ensure that any critical services that were impacted by the deletions are functioning properly after restoration.
3. **Enhance Monitoring:**
   * Implement enhanced monitoring on registry changes to detect any future unauthorized modifications. This can include configuring syscheck to monitor key registry paths closely.
   * Utilize alerts for any critical registry modifications to facilitate quicker responses.
4. **User Access Review:**
   * Review user permissions for accounts that have access to modify the registry. Limit permissions based on the principle of least privilege.
   * Ensure that only trusted administrative accounts can make changes to critical registry paths.
5. **Update Security Policies:**
   * Update incident response policies to ensure swift actions are taken when unauthorized changes are detected.
   * Conduct user training on security best practices and the importance of reporting suspicious behavior.

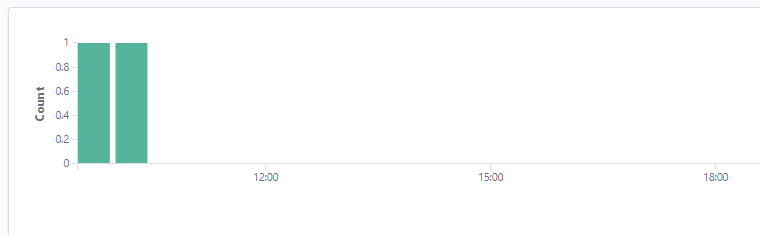
**VI. Compliance Alignment:**

1. **PCI DSS Compliance:**
   * Ensure compliance with PCI DSS requirement 11.5 by implementing continuous monitoring of critical system components for unauthorized changes.
   * Review access logs and security controls to ensure they align with PCI DSS standards.
2. **NIST 800-53 Compliance:**
   * Align with NIST 800-53 SI.7 by ensuring that the organization implements appropriate measures to detect unauthorized changes in the system.
   * Regularly review and update security controls based on the latest NIST guidelines.
3. **GDPR Compliance:**
   * Ensure that any personal data handled by the affected services complies with GDPR requirements, particularly in terms of data integrity and protection.

**VII. Further Steps:**

1. **Follow-Up Audit:**
   * Schedule a follow-up audit to assess the effectiveness of remediation measures and confirm that unauthorized changes have been fully addressed.
   * Re-evaluate security measures based on findings from this incident to enhance overall security posture
2. **Review Incident Response Plan:**
   * Reassess and update the incident response plan to ensure that it includes specific procedures for handling unauthorized registry changes.
   * Conduct tabletop exercises to prepare the incident response team for similar future incidents.

**2. High amount of POST request in a small amount of time.**

****

**Figure 2: High amount of POST request in a small amount of time.**

**I. Alert Description:**

* **Level**: 10 (High Severity)
* **Description**: High amount of POST requests in a small period of time (likely bot).
* **Groups**: web, appsec, attack

**II. Rule Information:**

* **Rule ID**: T1498
* **Mail Notification:** No
* **Compliance Standards:**
  + PCI DSS: 6.5, 11.4
  + **HIPAA:** 164.312.c.1, 164.312.c.2
  + TSC: CC6.6, CC7.1, CC8.1, CC6.1, CC6.8, CC7.2, CC7.3
  + NIST 800-53: SA.11, SI.4
  + GDPR: IV\_35.7.d

**III. Alert Details:**

* **Location**: /var/log/apache2/access.log
* **Decoder**: web-accesslog
* **Agent** **Information**:
  + **IP**: 10.0.11.135
  + **Name**: eklas.jgu.ac.id
  + **ID:** 202
* **Source IP**: 172.71.124.220, 172.71.210.233
* **Full Log:**
  + - 172.71.210.233 - - [10/Oct/2024:10:21:21 +0800] "POST /att/index.php?center=jgu\_main&sess\_id=MjAyNDA5MDAwMTE1NQ== HTTP/1.1" 200 341 "https://klas.jgu.ac.id/att/index.php?center=jgu\_main&sess\_id=MjAyNDA5MDAwMTE1NQ==" "Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.0.0 Mobile Safari/537.36" File '/etc/nginx/conf.d/www.msumedicalcentre.com.conf' modified Mode: scheduled Changed attributes: inode,mtime Old modification time was: '1728035932', now it is '1728448743' Old inode was: '53871924', now it is '53872566'
    - 172.71.124.220 - - [10/Oct/2024:09:42:21 +0800] "POST /att/index.php?center=jgu\_main&sess\_id=MjAyNDA5MDAwMTE1NQ== HTTP/1.1" 200 342 "https://klas.jgu.ac.id/att/index.php?center=jgu\_main&sess\_id=MjAyNDA5MDAwMTE1NQ==" "Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.0.0 Mobile Safari/537.36"
  + **Ticket ID**: NA

**IV. Significant Findings and Impact:**

* **Event Type:** Potential Web Application Attack
* **Observation:** A significant number of POST requests originating from multiple IP addresses within a short time frame suggests automated behavior, commonly associated with bots or malicious actors attempting to exploit the application.
* **Impact:**
  + High volume of requests can lead to performance degradation or service denial for legitimate users.
  + Potential data breaches or exploitation of vulnerabilities if the application is susceptible.
  + Increased risk of resource exhaustion, affecting the overall availability of services.

**V. Remediation Measures:**

1. **Rate Limiting:**
   * Implement rate limiting on the server to control the number of requests from a single IP address within a specified timeframe. This will help mitigate potential bot attacks.
2. **Web Application Firewall (WAF):**
   * Deploy a Web Application Firewall to filter and monitor HTTP requests. The WAF can help identify and block suspicious traffic patterns, including excessive POST requests.
3. **Bot Management Solutions:**
   * Consider integrating bot management solutions that can differentiate between legitimate user traffic and bot traffic. This may involve using CAPTCHA or JavaScript challenges for suspected bot behavior.
4. **Log Analysis:**
   * Continuously monitor and analyze access logs for unusual patterns or spikes in traffic. Automate alerts for anomalous behavior to enable prompt investigation.
5. **Patch and Secure the Application:**
   * Review the application for vulnerabilities and ensure that all components are updated and patched against known exploits.
   * Conduct a security assessment or penetration test to identify and remediate any weaknesses in the application.

**VI. Compliance Alignment:**

1. **PCI DSS Compliance:**
   * Ensure compliance with PCI DSS requirements 6.5 and 11.4 by maintaining secure applications and protecting against unauthorized access and vulnerabilities.
   * Implement logging mechanisms to track access and modifications to sensitive data.
2. **HIPAA Compliance:**
   * Align with HIPAA requirements 164.312.c.1 and 164.312.c.2 by ensuring that patient data is protected against unauthorized access and that access logs are maintained.
3. **NIST 800-53 Compliance:**
   * Ensure compliance with NIST controls SA.11 and SI.4 by implementing continuous monitoring and vulnerability management practices.
4. **GDPR Compliance:**
   * Align with GDPR requirements IV\_35.7.d by ensuring that data processing activities are transparent and that users can request information about data collection.

**VII. Further Steps:**

1. **Incident Review:**
   * Conduct a post-incident review to analyze the attack vector and evaluate the effectiveness of the implemented remediation measures.
2. **Training and Awareness:**
   * Provide training to development and IT staff on secure coding practices and the importance of application security. Raise awareness of the potential impact of automated attacks.

**Executive Summary:**

1. **Registry Value Entry Deleted:**

**Alert Details:**

* + **Location:** HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\MpKsl4dc81977
  + **Agent Information:**
    1. **IP:** 10.0.16.52, 10.0.16.53, 10.0.16.47
    2. **Name:** app1.msumedicalcentre.com, app2.msumedicalcentre.com, db3.msumedicalcentre.com
    3. **ID:** 009, 010, 008
  + **Full Log:**
    1. Registry values deleted from critical system paths indicate potential unauthorized access.
  + **Ticket ID:** NA

**Significant Findings and Impact:**

* + **Event Type:** Defense Evasion
  + **Observation:** Multiple registry value deletions suggest potential malicious activity affecting system services.
  + **Impact:** Compromised system stability and increased risk of unauthorized actions.

**Remediation Measures:**

* + Conduct a thorough investigation of the deletions and review logs for suspicious activity.
  + Restore deleted registry values from backups if unauthorized.
  + Enhance monitoring of registry changes and review user access permissions.

**Further Steps:**

* + Schedule a follow-up audit to assess remediation effectiveness.
  + Update incident response policies and conduct user training on security best practices.

1. **High Amount of POST Requests in a Short Time:**

**Alert Details:**

* + **Location:** /var/log/apache2/access.log
  + **Decoder:** web-accesslog
  + **Agent Information:**
    1. **IP:** 10.0.11.135
    2. **Name:** eklas.jgu.ac.id
    3. **ID:** 202
  + **Source IP:** 172.71.124.220, 172.71.210.233
  + **Full Log:**
    1. Multiple POST requests detected within a short timeframe, indicating potential automated behavior.
  + **Ticket ID:** NA

**Significant Findings and Impact:**

* + **Event Type:** Potential Web Application Attack
  + **Observation:** High volume of POST requests suggests automated attacks possibly aimed at exploiting application vulnerabilities.
  + **Impact:** Risk of service degradation, data breaches, and increased resource exhaustion.

**Remediation Measures:**

* + Implement rate limiting to control request volumes from individual IPs.
  + Deploy a Web Application Firewall (WAF) to monitor and filter suspicious traffic.
  + Conduct ongoing log analysis to detect and respond to anomalous behavior.

**Further Steps:**

* + Conduct a post-incident review to evaluate attack vectors and response effectiveness.
  + Provide training for staff on secure coding practices and the implications of automated attacks.

### Conclusion

The alerts indicate critical vulnerabilities that necessitate immediate attention. Timely investigations, robust remediation measures, and ongoing monitoring will help safeguard the integrity of MSU Medical Centre's systems and protect against future threats.