Systems with the update service disabled

Keeping up with patch maintenance is a critical part of effective cyber-hygiene. Windows-based systems are especially at risk when unpatched, considering the number and frequency of exploits that use Windows vulnerabilities to establish a foothold, move laterally, or propagate. Windows-based systems that stop updating may be the target of malicious activity. However, the same type of event may simply be the result of an environmental change, other configuration issue on the host, or scheduled downtime. If the update service itself is disabled on the host, then it may indicate a compromised system. You want to search for disabled update capabilities.

Required data

**System log data.** This sample search uses Windows event logs. You can replace this source with any other system log data used in your organization.

Procedure

1. Identify all relevant IT assets from a data mapping exercise conducted by the Data Privacy Officer’s team. These are all IT assets that are relevant to the full audit trail of data processing activities. This includes not only data stores and repositories that house sensitive personal data (PD) and personally identifiable information (PII), but also any technologies that are involved in the processing, storage, transmission, receipt, rendering, encrypt/decrypt, relaying, and handling of such data in any capacity.

2. Ensure that those assets are configured properly to report logging activity to an appropriate central repository.

3. Use your data mapping results to build a lookup that associates systems to their system category. At a minimum, the lookup must contain the host field mapped to a GDPR (or other compliance) category.

4. Run the following search. You can adjust this query based on the specifics of your environment.

```
| (sourcetype=wmi:service OR (source=winhostmon Type=Service) OR (tag=service tag=os)) (tag=update OR Name=wuauserv) StartMode!=Auto 
|bucket _time span=1d 
|stats latest(Status) AS Status latest(StartMode) AS StartMode by _time host Name 
|lookup <name of lookup you created in step 3> host 
|search category=* 
|stats earliest(_time) as earliest latest(_time) AS latest BY StartMode, host 
|where earliest > relative_time(now(), "-1d@d")
```

Search explanation

The table provides an explanation of what each part of this search achieves. You can adjust this query based on the specifics of your environment.

---

The information provided in Splunk Lantern is intended for informational and educational purposes only. All information is provided in good faith, however, Splunk disclaims any and all representations and warranties, express and implied, regarding the information provided, including without limitation any warranties and representations regarding the completeness, adequacy or accuracy of the information. You agree to take full responsibility for the results arising from the use of the information provided.
<table>
<thead>
<tr>
<th>Splunk Search</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>(sourcetype=wmi:service OR (source=winhostmon Type=Service) OR (tag=service tag=os)) (tag=update OR Name=wuauserv)</td>
<td>Search for various known sources, tags and source types for endpoint update and or patch service events.</td>
</tr>
<tr>
<td>StartMode!=Auto</td>
<td>Search for where the service doesn't start automatically.</td>
</tr>
<tr>
<td></td>
<td>bucket _time span=1d</td>
</tr>
<tr>
<td></td>
<td>stats latest(Status) AS Status latest(StartMode) AS StartMode by _time host Name</td>
</tr>
<tr>
<td></td>
<td>lookup &lt;name of lookup you created in step 3&gt; host</td>
</tr>
<tr>
<td></td>
<td>search category=*</td>
</tr>
<tr>
<td></td>
<td>stats earliest(_time) as earliest latest(_time) AS latest BY StartMode, host</td>
</tr>
<tr>
<td></td>
<td>where earliest &gt; relative_time(now(), &quot;-1d@d&quot;)</td>
</tr>
</tbody>
</table>

**Next steps**

Identify the in-scope systems where updates are not occurring, pinpoint the root issue for updates not occurring, and remediate those hosts by configuring them or the environment appropriately, depending on what the root issue turns out to be. When an update service is disabled, the immediate question is why. Ask the user if they disabled it, look for software installations that might have done it, or look for any errors related to the Windows Update Service (wuauserv.exe).

Additionally, you should monitor the mapped IT assets changes in logging status, adjust for known outages, and...
prioritize incident response for any failures to report by hosts that are not scheduled for downtime.

**GDPR Relevance:** Unpatched systems put data at risk. For any unpatched environments/systems that are involved in processing personal data, this situation can be critical, and especially so in a GDPR context, since any GDPR-tagged systems not receiving updates could jeopardize a state of compliance. GDPR Article 32 requires that you regularly test, assess and evaluate the effectiveness of your implemented technical and organizational security controls. If the Authority executes its powers and your Organization is in the scope of a privacy audit, you need to demonstrate compliance (Article 58). Also, in case you face a breach and individuals are impacted, they have the right to compensation of the damage. If an organization can prove that they have done everything appropriate to the risk and deployed proper countermeasures, they shouldn't be liable (Article 82). Ensuring patches are applied to your systems is industry best practices and state of the art.

Finally, you might be interested in other processes associated with the [Complying with General Data Protection Regulation](#) use case.