Threat-Hunting

Queries Pack for the Oracle EBS Zero-Day (CVE-2025-61884 & CVE-2025-61882)

How to use

1. **Pick your Platform** - Splunk, Microsoft Sentinel, or Elastic.
2. **Copy the query** from the relevant card.
3. **Replace placeholders** like INDEX_WEB, INDEX_SYS, MGMT_CIDR, ALLOWLIST_IPS, EBS_HOSTS[], ORACLE_IOCS[]
4. **Run as ad-hoc hunt first**; convert to scheduled alert after tuning.

0) Quick IOC seeds (set once and reuse)

Splunk (lookup macro-style vars)

```
| makeresults
| eval EBS_PATHS="/OA_HTML/configurator/UiServlet,/OA_HTML/SyncServlet",
    ORACLE_IOCS="185.181.60.11,200.107.207.26",
    ALLOWLIST_IPS="10.0.0.0/8,172.16.0.0/12,192.168.0.0/16"
```

Sentinel (KQL let)

```
let EbsPaths = dynamic(["/OA_HTML/configurator/UiServlet","/OA_HTML/SyncServlet"]);
let OracleIocs = dynamic(["185.181.60.11","200.107.207.26"]);
let AllowListCidrs = dynamic(["10.0.0.0/8","172.16.0.0/12","192.168.0.0/16"]);
let EbsHosts = dynamic(["ebs-app1","ebs-app2"]); // optional| project TimeGenerated, HostName, user, src_ip, SyslogMessage
| invoke _GetGeoInfo(src_ip)
| summarize by TimeGenerated, HostName, user, src_ip, Country, City
```

Elastic (Saved search params)

- ebs.paths: ("/OA_HTML/configurator/UiServlet" OR "/OA_HTML/SyncServlet")
- Add runtime filters for IP allowlist and host names.

1) Web access to vulnerable endpoints (UiServlet / SyncServlet)

Splunk (Apache/HTTP Server / WebLogic OHS)

```
index=INDEX_WEB sourcetype IN (apache:access, http_access, weblogic:access)
(uri_path="/OA_HTML/configurator/UiServlet" OR uri_path="/OA_HTML/SyncServlet")
| eval is_allowlisted=if(cidrmatch("ALLOWLIST_IPS", src_ip), 1, 0)
| stats count AS hits, earliest(_time) AS first_seen, latest(_time) AS last_seen BY host, src_ip, http_method, uri_path, status, useragent
| where is_allowlisted=0 OR status IN (200,302,500)
| sort - last_seen
```

Sentinel (CommonSecurityLog / WAF / AppGW)

```
CommonSecurityLog
| where RequestURL has "/OA_HTML/"
| where RequestURL has_any ("configurator/UiServlet","SyncServlet")
| extend Path = tostring(url_decode(RequestURL))
| where not(ipv4_is_private(SourceIP))
| summarize hits=count(), first_seen=min(TimeGenerated), last_seen=max(TimeGenerated) by DeviceName, SourceIP, RequestClientApplication, RequestURL, HttpRequestMethod, DestinationPort
| order by last_seen desc
```

Elastic

```
(event.dataset: "apache.access" OR http.request.method:*)
AND url.path: ("/OA_HTML/configurator/UiServlet" OR "/OA_HTML/SyncServlet")
AND NOT source.ip: (10.0.0.0/8 OR 172.16.0.0/12 OR 192.168.0.0/16)
```

2) Suspicious query strings / SSRF indicators (return_url, unusual redirects)

SPLUNK (SPL)

```
index=INDEX_WEB sourcetype IN (apache:access, http_access, weblogic:access)
uri_path="/OA_HTML/configurator/UiServlet"
| rex field=uri_query "(?<return_url>return_url=[^&]+)"
| search return_url=*
| eval ext_host=mvindex(split(urldecode(return_url),"//"),1)
| where NOT like(ext_host,"%yourdomain%")
| table _time, host, src_ip, http_method, uri_path, uri_query, ext_host, useragent, status
| sort - _time
```

Microsoft Sentinel (KQL)

```
CommonSecurityLog
| where RequestURL has "configurator/UiServlet"
| extend q=parse_url(RequestURL).QueryString
| extend return_url=iff(tostring(q) has "return_url", tostring(q), "")
| where return_url != ""
| extend decoded=urldecode(RequestURL)
| project TimeGenerated, DeviceName, SourceIP, RequestClientApplication, RequestURL, decoded
```

Elastic (KQL)

```
url.path: "/OA_HTML/configurator/UiServlet" AND url.query: "*return_url=*"
```

3) Known malicious source IPs or abnormal geos

SPLUNK (SPL)

```
index=INDEX_WEB sourcetype IN (apache:access, http_access, weblogic:access)
(uri_path="/OA_HTML/configurator/UiServlet" OR uri_path="/OA_HTML/SyncServlet")
| lookup oracle_iocs.csv ip OUTPUT ip AS hit
| eval from_ioc=if(isnotnull(hit),1,0)
| iplocation src_ip
| stats count BY host, src_ip, Country, uri_path, status
| where from_ioc=1 OR (Country!="YourCountry" AND count>0)
```

Microsoft Sentinel (KQL)

```
CommonSecurityLog
| where RequestURL has_any ("configurator/UiServlet","SyncServlet")
| where SourceIP in (OracleIocs) or isnotempty(SourceIP)
| invoke _GetGeoInfo(SourceIP)
| summarize hits=count() by DeviceName, SourceIP, Country, RequestURL
```

Elastic (KQL)

```
url.path:(*UiServlet OR *SyncServlet) AND source.ip:(185.181.60.11 OR 200.107.207.26)
```

4) Reverse shell & suspicious command execution on EBS hosts

Splunk (Linux audit/syslog)

```
index=INDEX_SYS host IN (EBS_HOSTS)
( (process="bash" OR cmdline="bash*") AND cmdline="* /dev/tcp/*" )
OR (cmdline="*bash -i* >& */dev/tcp/* 0>&1*")
| table _time, host, user, process, cmdline, parent_process
| sort - _time
```

Sentinel (Syslog / AMA)

```
Syslog
| where HostName in (EbsHosts)
| where SyslogMessage has_any ("/dev/tcp/","bash -i"," >& ")
| project TimeGenerated, HostName, ProcessName, SyslogMessage
| order by TimeGenerated desc
```

Elastic (KQL)

```
host.name:(ebs-app1 OR ebs-app2) AND process.command_line:(*"/dev/tcp/"* OR *"bash -i"* )
```

5) Unusual outbound egress from EBS to the internet (exfil/C2)

Splunk (NetFlow/Zeek)

```
index=INDEX_NET sourcetype IN (zeek:conn, netflow)
src_ip IN (MGMT_CIDR) OR src_host IN (EBS_HOSTS)
| stats sum(bytes_out) AS out_bytes, count AS conns BY src_ip, dest_ip, dest_port
| where out_bytes > 500000000 OR conns > 200
| sort - out_bytes
```

Sentinel (NSG Flow / Firewall)

```
AzureNetworkAnalytics_CL
| where SrcIp_s in (EbsHosts) or SrcIp_s matches regex @"^10\.X\."
| summarize bytes_out=sum(BytesSent_d), conns=count() by SrcIp_s, DstIp_s, DstPort_d
| where bytes_out > 5e8 or conns > 200
| order by bytes_out desc
```

Elastic (Zeek/Netflow)

```
source.address:(EBS_HOSTS OR MGMT_CIDR) AND NOT destination.ip:(10.0.0.0/8 OR 172.16.0.0/12 OR 192.168.0.0/16)
```

6) Dropped webshells / rogue files under $OA_HTML (JSP/class)

SPLUNK (SPL)

```
index=INDEX_SYS host IN (EBS_HOSTS) sourcetype=fschange
path="/u01/app/ebs/apps/apps_st/appl/fnd/12.0.0/portal/web/*"
| search (file_ext="jsp" OR file_ext="class" OR file_ext="war")
| stats values(action) AS actions, earliest(_time) AS first_seen, latest(_time) AS last_seen BY host, path, file_hash
```

Sentinel (File integrity via AMA / Defender for Servers)

```
SecurityAlert
| where Entities has_any ("jsp","class",".war") and Title has "file created"
| where tostring(todynamic(Entities)[0].HostName) in (EbsHosts)
```

Elastic (FIM)

```
file.extension:(jsp OR class OR war) AND file.path:/u01/*/OA_HTML/*
```

7) New local admin users or unexpected app changes

Splunk (DB/Config audit, syslog)

(Adjust to your EBS OS/user management source)

```
index=INDEX_SYS host IN (EBS_HOSTS) sourcetype=linux:secure
("useradd" OR "usermod" OR "groupadd") AND ("wheel" OR "sudo" OR "root")
| table _time, host, user, process, cmdline
```

Sentinel

```
Syslog
| where HostName in (EbsHosts)
| where SyslogMessage has_any ("useradd","usermod","groupadd") and SyslogMessage has_any ("wheel","sudo","root")
```

Elastic

```
host.name:(ebs-app1 OR ebs-app2) AND system.auth.ssh.message:(*useradd* OR *usermod*) AND system.auth.ssh.message:(*wheel* OR *sudo* OR *root*)
```

8) WAF blocks/alerts on the two servlet paths

SPLUNK (WAF)

```
index=INDEX_WAF (uri="/OA_HTML/configurator/UiServlet" OR uri="/OA_HTML/SyncServlet")
| stats count BY action, src_ip, uri, rule_id, host
| sort – count
```

Sentinel (WAF logs)

```
AzureDiagnostics
| where Category in ("ApplicationGatewayFirewallLog","FrontDoorWebApplicationFirewallLog")
| where RequestUri_s has_any ("/OA_HTML/configurator/UiServlet","/OA_HTML/SyncServlet")
| summarize hits=count() by action_s, clientIp_s, RequestUri_s, ruleSetType_s, ruleId_s
```

Elastic (KQL)

```
event.dataset: waf.* AND http.request.referrer:("/OA_HTML/configurator/UiServlet" OR "/OA_HTML/SyncServlet")
```

9) Recon wave detection (sudden spikes to EBS endpoints)

SPLUNK

```
index=INDEX_WEB (uri_path="/OA_HTML/configurator/UiServlet" OR uri_path="/OA_HTML/SyncServlet")
| timechart span=15m count BY uri_path
| anomalydetection action=annotate
```

Sentinel

```
CommonSecurityLog
| where RequestURL has "/OA_HTML/"
| summarize hits=count() by bin(TimeGenerated, 15m), RequestURL
| render timechart
```

Elastic

```
url.path:(*UiServlet OR *SyncServlet)
| stats count by @timestamp, url.path
```

Disclaimer

The materials, documents, and tools shared by Point Break Security GmbH and The Daily Signal channel are provided free of charge for the purpose of supporting and educating our audience.

While every effort is made to ensure accuracy and usefulness, Point Break Security GmbH, The Daily Signal, and any individual involved in producing or distributing this content do not guarantee the quality, accuracy, or suitability of the information or materials provided.

We cannot be held responsible or liable for any damages, losses, or issues that may arise from the use, misuse, or interpretation of these materials.

Users are solely responsible for verifying that any scripts, configurations, or recommendations are compatible with their own environment and for thoroughly testing them in a controlled or non-production setting before applying them to live systems.

By using these materials, you acknowledge that you do so at your own risk and accept full responsibility for how they are implemented.