Rapid Patch & Defense Checklist

Oracle EBS Zero-Day

Immediate actions

- ☐ **Apply Oracle patches for CVE-2025-61882 (RCE) and CVE-2025-61884 (SSRF)** - Both flaws form the full exploit chain — patching only one still leaves you exposed.
- ☐ **Confirm prerequisites (July 2023/Oct 2023 CPU installed)** - Required for the emergency fixes to apply cleanly.
- ☐ **Remove Oracle EBS from public internet** – Prevents direct exploitation of the UiServlet/SyncServlet endpoints. Access only via VPN or internal network.
- ☐ **Deploy temporary WAF rule** to block: */OA_HTML/SyncServlet* and */configurator/UiServlet* – Stops exploit traffic targeting known vulnerable endpoints.
- ☐ **Rotate credentials and API keys** related to Oracle EBS - If attackers probed your instance, they may have captured stored credentials.
- ☐ **Back up and snapshot before patching** – Ensures safe rollback and preserves forensic evidence if compromise is suspected.

Detection & Monitoring (Next 48 Hours)

- ☐ **Check Web server logs (access_log, error_log)** - Requests to /OA_HTML/configurator/UiServlet or /OA_HTML/SyncServlet, especially with strange query strings or from unknown IPs.
- ☐ **Source IPs from Oracle IOC list** - e.g. 185.181.60[.]11, 200.107.207[.]26 — any hits are red flags.
- ☐ **Shell execution traces** – Patterns like bash -i >& /dev/tcp/... or unusual child processes under the EBS app user.
- ☐ **Outbound traffic monitoring**: Unexpected data transfers or new connections from EBS servers to external IPs.
- ☐ **Integrity of web directories ($FND_TOP, $OA_HTML)** - Unrecognized .jsp or .class files may indicate dropped webshells.
- ☐ **SIEM / IDS rules** – Add alerts for “SyncServlet” and “UiServlet” in URI fields; flag non-whitelisted admin logins or config changes.

Long-Term Hardening (Next 30 Days)

- ☐ **Restrict EBS exposure permanently** - Require VPN or Zero-Trust proxy for all administrative access.
- ☐ **Implement continuous patch cadence** - Sync with Oracle's quarterly Critical Patch Updates (CPUs).
- ☐ **Enable audit logging and centralized monitoring** – Collect HTTP, database, and OS logs into a SIEM for correlation and long-term analysis.
- ☐ **Run regular ERP-focused pen tests** - Identify web-facing weaknesses before attackers do.
- ☐ **Review backup & DR strategy** - Ensure backups are offline, tested, and immutable in case of future extortion attempts.
- ☐ **Educate executives on extortion tactics** – Prepare comms and legal response plans to reduce panic during potential ransom outreach.

Quick Verification Commands

- ☐ **Linux grep example for suspicious access**
  - grep -E "UiServlet|SyncServlet" /var/log/httpd/access_log* | grep -v "internal_IPs"
- ☐ **Network check for outbound shells**
  - netstat -antp | grep :4444
- ☐ **WAF block example (ModSecurity concept)**
  - SecRule REQUEST_URI "@beginsWith /OA_HTML/SyncServlet" "id:1001,deny,status:403,msg:'Blocked Oracle EBS exploit attempt'"

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.