Confidential

GOVERNMENT OF PAKISTAN
NCERT
******

No.1-1/2025/DG (NCERT)/ 566 **Islamabad, the 29th October , 2025**

From

Dr Haider Abbas
DG -(nCERT)

To

1- MD, Khyber Pakhtunkhwa Information Technology Board KPITB,
2- Secretary, Science and Technology Balochistan,
3- Director CE and C Ex JIO Branch, JS HQ MoD,
4- Chief Secretary KPK, Govt of Khyber Pakhtun Khawa,
5- Chief Secretary Sindh, Govt of Sindh,
6- Cheif Secretary AJK, Govt of Azad Jammu and Kashmir,
7- Chief Secretary Punjab, Govt of Punjab,
8- Chief Secretary GB, Govt of Gilgit Baltistan,
9- Chief Secretary Balochistan, Govt of Balochistan,
10- CISO, Nadra,
11- Chairman, PAEC, PAEC near K-Block P.O Box 1114 Pak Secretariat Islamabad.
12- Director General, NECOP, NECOP Street Number 6 Sector H-9 I Islamabad.
13- Chair Main, Punjab Information Technology Board PITB Government of Punjab,
14- DS, Information Technology Department Gilgit Baltistan Government of Gilgit Baltistan,
15- Governor, State Bank of Pakistan,
16- CISO, Punjab Information Technology Board PITB Government of Punjab,
17- Secretary Information, Science and Technology Department Government of Sindh,
18- Policy Expert Non Traditional Security, National Security Division,
19- DG, Information and Science and Technology Department Government of Sindh,
20- DG, Information Technology Board Government of Azad Jammu and Kashmir,
21- Secretary, Information Technology Department Gilgit Baltistan Government of Gilgit Baltistan,
22- Chairman PTA, PTA, Islamabad
23- Acting Chairman HEC, HEC, Islamabad
24- Cabinet Secretary, CAB, Islamabad
25- Chairman, NTCOMM, Islamabad
26- Chairman, SECP, NIC Building 63 Jinnah Avenue Blue Area Islamabad
27- Chairman NEPRA, NEPRA, Islamabad
28- Chairman OGRA, OGRA, Islamabad
29- Chief (Water Resources), PC, Islamabad
30- Chief of Staff, NADRA, Islamabad
31- DS EXP (Religious Affair/NFSR/BOI, MOF, Islamabad
32- Deputy Chief-I (Industries & Commerce), PC, Islamabad

33- Deputy Director Wafaqi Mohtasib, MONHS, Islamabad
34- Director General, PCAA, Karachi
35- Director General - Admin, NITB, Islamabad
36- Director General FIA, FIA, Islamabad
37- Federal Minister (Communication), MOCM, Islamabad
38- Federal Secretary of MoNHS, MONHS, Islamabad
39- Foreign Secretary, MOFA, Islamabad
40- GM (Human Resource), PPMC, Islamabad
41- Governor, State Bank of Pakistan, State Bank of Pakistan I.I. Chundrigar Road Karachi
42- Joint Executive Director III (Liquefied Petroleum Gas), OGRA, Islamabad
43- Parliamentary Secretary, MOC, Islamabad
44- SAPM for Industries & Production Division, MOIP, Islamabad
45- Secretary Climate Change, MOCC, Islamabad
46- Secretary General(National Assembly), NAS, Islamabad
47- Secretary IT, MoIT, Islamabad
48- Secretary Kashmir Affair,Gilgit Baltistan & SAFRON, kagbsafron, Islamabad
49- Secretary LAW & Justice, MOLJ, Islamabad
50- Secretary Planning, PC, Islamabad
51- Secretary Revenue Div/Chairman FBR, FBR, Islamabad
52- Secretary of Interior, MOINC, Islamabad

SUBJECT: <u>CYBERSECURITY ADVISORY ON IMMEDIATE MITIGATION OF ORACLE E-BUSINESS SUITE (EBS) EXPLOITATION CAMPAIGN</u>

In view of the recently identified critical vulnerability in Oracle eBusiness Suite (EBS), which is being actively exploited by cyber threat actors for unauthorized access, data theft, and extortion campaigns, the attached Advisory titled "*NCA-13.281025 – National CERT Advisory – Critical Remote Code Execution Vulnerability in Oracle eBusiness Suite (EBS)*" **(Annexure)** has been issued by the National Cyber Emergency Response Team (National CERT).

2. The advisory details the nature, risks, and operational impacts of the ongoing exploitation campaign, which leverages the identified vulnerability to execute privileged tasks without authentication on unpatched Oracle EBS systems. Exploitation of this flaw may result in complete system compromise, exfiltration of sensitive business or government data, and service disruption. Given the extensive use of EBS across Government, Military, and critical infrastructure organizations, the threat is of immediate and critical concern. The document further provides detailed mitigation guidance, including urgent patching instructions, network isolation measures, monitoring recommendations, and incident response steps to detect and contain potential compromise. Organizations are strongly advised to apply Oracle's latest security updates, restrict public access to EBS systems, and review system logs for any signs of unauthorized activity.

3. It is requested that the attached Advisory be disseminated to all concerned departments and organizations under your administrative purview. Immediate action is required to mitigate potential exploitation and ensure continued operational security of Oracle EBS environments.

Annexure: NCA-13.281025 – National CERT Advisory – Critical Remote Code Execution Vulnerability in Oracle eBusiness Suite (EBS)

Dr Haider Abbas
DG -(nCERT)
Ph:03009634911

Annexure

NCA-13.281025 – National CERT Advisory – Critical Remote Code Execution Vulnerability in Oracle eBusiness Suite (EBS)

1. Introduction

A critical vulnerability has been identified in Oracle eBusiness Suite (EBS) that enables unauthenticated remote code execution (RCE) and allows attackers to perform privileged tasks without authentication. This flaw is currently being actively exploited in the wild by cyber threat actors to conduct data theft, extortion, and ransom campaigns targeting enterprise and government EBS environments.

Successful exploitation grants attackers full administrative control over the EBS system, enabling unauthorized access, data exfiltration, and service disruption. Given EBS's integral role in managing financial, supply chain, and HR operations, compromise of this system poses severe operational, financial, and reputational risks particularly for Government and Military institutions utilizing the platform.

2. Impact

Successful exploitation may result in:

a. **Remote Code Execution (RCE)** – Execution of arbitrary commands with elevated privileges.
b. **Unauthorized Access** – Full control over Oracle EBS environments.
c. **Data Theft** – Exfiltration of sensitive business, financial, or regulated data.
d. **Service Disruption** – Interruption of core business and operational processes.
e. **Extortion and Reputational Damage** – Threat of data exposure or ransom demands.
f. **Legal and Compliance Exposure** – Due to data breach notification obligations.

3. Threat Details

i. Vulnerability Overview:

CVE ID	Affected Product(s)	Description	CVSS v3.1	CWE
TBD (Pending Oracle Disclosure)	Oracle eBusiness Suite (EBS)	Unauthenticated remote code execution allowing privileged task execution and data exfiltration	9.8 (Critical)	CWE-306 (Missing Authentication for Critical Function)

ii. Attack Complexity & Vector:

a. **Attack Vector:** Remote (HTTP/HTTPS access to exposed EBS services)
b. **Attack Complexity:** Low
c. **Privileges Required:** None
d. **User Interaction:** Not required
e. **Exploitation Status:** Active exploitation confirmed in the wild

4. Affected Systems

a. The following configurations are considered vulnerable if unpatched or exposed:
b. Any Oracle EBS instance accessible over the internet or from untrusted networks.
c. Systems not updated with the latest Oracle Critical Patch Update (CPU).
d. EBS deployments without network segmentation or perimeter protection.
e. Outdated or unsupported EBS versions still in operational use.
f. Government or Military systems connected to shared or hybrid infrastructure.

5. Exploit Conditions

Successful exploitation may require:

a. Network access to externally exposed Oracle EBS web or application services.
b. Lack of enforced authentication or MFA for privileged endpoints.
c. Absence of recent Oracle security updates.
d. Inadequate network segmentation or firewall rules.

6. Recommendations & Mitigation Actions

i. Apply Patches Immediately (Recommended Fix)

a. Deploy the latest Oracle Critical Patch Update (CPU) addressing this vulnerability.
b. Confirm all prerequisite patches are installed.
c. Validate patch installation through Oracle EBS diagnostic utilities.
d. **Reference**: Oracle Security Alerts CVE-2025-61882

ii. Restrict External Exposure

a. Temporarily disable external access to Oracle EBS systems.
b. Place EBS behind firewalls, VPNs, or application gateways.
c. Block unnecessary ports and protocols associated with EBS.
d. Ensure no direct internet exposure of EBS management interfaces.

iii. Monitor for Indicators of Compromise (IoCs)

a. Review system and application logs for unusual activity or authentication bypass attempts.
b. Enable and fine-tune endpoint detection and response (EDR) and network monitoring tools.
c. Monitor for suspicious data transfers or large outbound connections.

iv. Strengthen Access Controls

a. Enforce multi-factor authentication (MFA) for all administrative accounts.
b. Rotate credentials and service account passwords linked to EBS.
c. Review role-based access controls (RBAC) to ensure least privilege.

v. Backup and Recovery Readiness

a. Ensure recent, offline, and tested backups of EBS databases and configurations exist.
b. Validate integrity and security of backup data prior to restoration.

vi. Incident Response and Escalation

a. Activate the organization's incident response plan if compromise is suspected.
b. Isolate affected systems to prevent further propagation.
c. Preserve forensic evidence (logs, memory, network captures).
d. Engage forensic and cybersecurity specialists as required.

vii. Monitoring & Detection

Organizations should:

a. Inspect EBS logs for unauthorized access or unexpected administrative actions.
b. Correlate Oracle EBS logs with SIEM systems for anomaly detection.
c. Monitor for suspicious file uploads, command executions, or data exfiltration attempts.
d. Analyze network traffic for connections to known malicious IPs or C2 infrastructure.

7. Patching Summary

Version Category	Affected Components	Status
Vulnerable	Unpatched Oracle EBS deployments	Must patch immediately
Secure	Systems updated with Oracle's latest Critical Patch Update	No further action required

8. References:

1. "CrowdStrike Identifies Campaign Targeting Oracle E-Business Suite via Zero-Day Vulnerability (now tracked as CVE-2025-61882)" – CrowdStrike blog. https://www.crowdstrike.com/en-us/blog/crowdstrike-identifies-campaign-targeting-oracle-e-business-suite-zero-day-CVE-2025-61882/

2. "Active exploitation of vulnerability affecting Oracle E-Business Suite" – National Cyber Security Centre (NCSC) advisory. https://www.ncsc.gov.uk/news/active-exploitation-vulnerability-affecting-oracle-ebusiness-suite

9. Call to Action

The National CERT advises all organizations to:

a. Immediately apply Oracle's latest security updates to all EBS environments.
b. Restrict network exposure by placing EBS behind secure network perimeters.
c. Continuously monitor for compromise indicators or unauthorized access attempts.
d. Integrate this vulnerability into organizational patch and risk management workflows.