DAYANANDA SAGAR COLLEGE OF ENGINEERING
An Autonomous Institute Affiliated to VTU, Belagavi Approved by AICTE ; ISO 9001:2015 Certified
Accredited by National Assessment Accreditation Council (NAAC) with 'A' grade
Shavige Malleshwara Hills, Kumaraswamy Layout, Bengaluru-560078

Department of Artificial Intelligence & Machine Learning

Incident Identification		
Submitted By: Aditi Sharma – Data Protection Officer (DPO)	**Date & Time:** 20 October 2025, 08:45 AM IST	**Report Ref No:**DB-2025-01
Title: Unauthorized Access to Customer Database via Exposed API Token	**Company:** TechSecure Pvt. Ltd.	**System / Application:** Customer Management Portal (API Service – AWS Cloud)

Type of Incident Detected					
Denial of Service		**Malicious Code**		**Unauthorized Use**	
Unauthorized Access	**Detected**	**Unplanned**		**Other**	

Description:
On **20 October 2025**, the **Security Operations Center (SOC)** detected abnormal API activity involving multiple unauthorized access attempts from foreign IP addresses. Investigation revealed that an **API authentication token** had been **accidentally exposed in a public GitHub repository** during deployment. This exposure allowed unauthorized access to the customer database, compromising personal identifiable information (PII) of approximately **2,500 users**, including **names, email addresses, and phone numbers**. No passwords, financial, or biometric data were affected. The incident was reported to the **Data Protection Officer (DPO)** immediately, who initiated containment and recovery measures.

People Involved:		
Name	**Designation**	**Role in Incident**
Aditi Sharma	Data Protection Officer	Incident lead, reporting, and compliance
Rohit Nair	Chief Information Security Officer (CISO)	Oversaw containment and system security review
Rahul Verma	DevOps Engineer	Identified API exposure in code repository
Neha Iyer	Security Analyst	Performed log analysis and breach confirmation
Priya Singh	Communications Manager	Coordinated user and regulatory notifications

Others Notified
• Data Protection Board of India (Notified within 48 hours) • Senior Management & Legal Compliance Team • All 2,500 affected customers via registered email

Actions

Identification / Verification measures:

- Detected through automated API monitoring alerts and SOC anomaly reports.
- Verified through access logs confirming unauthorized queries from unrecognized IP addresses.

Containment measures:

- Revoked and regenerated all API tokens immediately.
- Blocked all suspicious IPs accessing the server.
- Disabled the exposed endpoint temporarily for review.

Evidence collected (system logs etc.)

- API access logs and timestamped user query data.
- GitHub commit logs showing token exposure timeline.
- Firewall traffic logs for forensic evidence.

Eradication measures:

- Removed exposed API keys from repositories.
- Implemented token encryption and automated secret scanning in CI/CD pipeline.
- Conducted security patching and vulnerability scanning of all systems.

Recovery measures:

- Restored the secure API service with new authentication mechanisms (OAuth 2.0).
- Validated system integrity and verified no data tampering.
- Conducted user communication and reassurance campaign.

Other mitigation measures:

- Introduced mandatory **DPO approval** for API deployments.
- Initiated periodic **developer cybersecurity training**.
- Enforced **90-day key rotation policy** across all environments.

Learning:

- Security checks must be integrated at every stage of the DevOps pipeline.
- Public repositories pose a critical data exposure risk if not monitored.
- Continuous employee awareness and automated secret detection are essential.
- Timely detection and reporting helped minimize regulatory and reputational impact.
- Strong data protection governance ensures compliance with **DPDP Act 2023** and **GDPR standards**.