Relatório Técnico Forense - Incidente de Segurança

1. Introdução

No dia 21 de Abril de 2025, foi detectado um incidente de segurança nos sistemas da organização, envolvendo tentativas de exploração de vulnerabilidades do tipo SQL Injection. Este relatório descreve a natureza do ataque, medidas tomadas, evidências coletadas e recomendações para mitigação.

2. Descrição Técnica do Ataque

Os registros da tabela 'semedapp_tipodemanda' indicam múltiplas tentativas de exploração SQL Injection, utilizando payloads como PG_SLEEP(15), WAITFOR DELAY '0:0:15', e DBMS_PIPE.RECEIVE_MESSAGE, que visam travar ou explorar o banco de dados, explorando possíveis falhas de validação de entrada.

3. Análise Detalhada

Foram encontrados 244 registros suspeitos entre 21:00h e 22:00h do dia do incidente. Esses registros foram inseridos em sequência rápida, indicando um ataque automatizado ou script.

4. Medidas Emergenciais Adotadas

- Backup imediato dos dados.
- Isolamento da aplicação.
- Identificação dos registros contaminados.
- Análise forense inicial.
- Planejamento de reforço de segurança.

5. Boas Práticas de Defesa

- Uso obrigatório de consultas parametrizadas (prepared statements).
- Validação e sanitização de todos os inputs.
- Uso de Web Application Firewall (WAF).
- Implementação de logs e alertas de segurança.
- Revisão periódica de código e acessos.

6. Checklist Pós-Incidente

- Reset de senhas administrativas.
- Auditoria completa de sessões e dispositivos.
- Reforço nas validações de formulários.
- Bloqueio de IPs suspeitos.
- Atualização de patches de segurança.

7. Preservação de Evidências

- Manter cópia íntegra dos logs de acesso e aplicação.
- Manter o banco de dados afetado sem alterações manuais.
- Documentar todas as ações tomadas.
- Gerar hashes dos arquivos de evidência para garantir integridade.
- Encaminhar as evidências às autoridades competentes.

8. Conclusão

O incidente foi detectado precocemente, permitindo a contenção inicial. As recomendações propostas devem ser implementadas com urgência para garantir a segurança do sistema e mitigar futuras tentativas de ataque.