Laboratório Avançado de Produção Pesquisa e Inovação em Software

Relatório #02 de atividade da equipe de segurança

Rodolfo Cabral Neves

Brasília, aos 19 de Julho de 2024

1. Introdução

Este presente documento consiste no relatório de atividades que compreendeu a semana de 15 a 19 de julho de 2024, cujo objetivo é apresentar as vulnerabilidades ou riscos encontrados, os impactos causados e as possíveis soluções e recomendações. O time é atualmente composto por Rodolfo Cabral Neves, e o escopo da atividade é os servidores do ambiente de homologação do projeto **Brasil Participativo – BP** e foram avaliadas as configurações Secure Shell - SSH dos servidores cujos IP's são 192.168.3.21 e 192.168.3.22. A metodologia usada foi *white-box.*

1. Riscos encontrados

Durante o processo de avaliação, foi identificado que os servidores possuem configurações de padrão de fábrica, o que consiste num risco, pois e eis alguns riscos possíveis:

- Ataques de força bruta/dicionário durante a autenticação
- Transporte de variáveis do ambiente do usuário para o servidor SSH, o que pode causar possíveis conflitos e anomalias
- Protocolos de autenticação ativos, que não serão utilizados como o Kerberos e Generic Security Services Application Program Interface - GSSAPI

2. Medidas de correção

Para a mitigação destes riscos, as configurações SSH do servidor foram atualizadas. Eis os campos atualizados:

```
LoginGraceTime 20
PermitRootLogin no # desabilitar o login do root
MaxAuthTries 6 # desabilitar ataque de força bruta
PermitEmptyPasswords no # desabilitar senhas vazias
KerberosAuthentication no # desabilitar autenticação por Kerberos
GSSAPIAuthentication no #desabilitar autenticação por GSSAPI
X11Forwarding no # desabilitar o servidor gráfico
PermitUserEnvironment no # desabilitar o transporte de variáveis do usuário
```

3. Conclusão

Configurações incorretas de segurança podem ser uma fonte de riscos de segurança de duas maneiras distintas. A primeira envolve configurações funcionais que afetam a segurança. A segunda está especificamente relacionada a configurações de segurança. Entretanto, é muito importante desativar serviços que não estão sendo utilizados e configurar corretamente os acessos dos usuários.