Presidência da República
Gabinete de Segurança Institucional
Departamento de Segurança da Informação e Comunicações
Centro de Tratamento de Incidentes de Redes do Governo

Alerta nº 03/2017 – Vulnerabilidade no Software Samba – CVE-2016-7494

1. Descrição do Problema

O *software* Samba permite a interoperabilidade de compartilhamento de arquivos e de impressoras entre platarformas Microtsoft Windows e outras plataformas, sejam elas UNIX, GNU/Linux, IBM System 390 e outros sistemas operacionais.

Clientes maliciosos podem realizar upload e executar no Servidor Samba códigos por meio de compartilhamentos que permitam escrita. Faz-se necessário, dada a vulnerabilidade identificar nas organizações, os dispositivos embarcados que possuem o Samba instalado.

De acordo com o time que mantem o Samba a vulnerabilidade está presente em **todas** as versões desde a 3.5.0 (1º de Março de 2010) até as versões anteriores a atualização do dia 24 de Maio de 2017.

2. Possíveis Riscos

O software sem o patch de correção pode ser explorado para comprometer a confidencialidade, integridade e disponibilidade das informações da organização sem necessidade de permissionamento adequado. Em outras palavras, a vulnerabilidade permite:

- Acesso às informações da organização;
- Modificação não autorizada de qualquer ativo de informação;
- Comprometimento de serviços;

3. Sugestão para Mitigação do Problema

Correção do software:

- Instalar uma das versões mais atuais do Samba 4.6.4, 4.5.10 ou 4.4.14 que foram disponibilizados para corrigir a falha.
- Como alternativa a instalação, aplicar o patch relacionado a esta falha também foi disponibilizado no sítio:

  `http://www.samba.org/samba/security/`

Mitigação:

- Caso não seja possível atualizar o software de forma imediata, é recomendável como forma de mitigar o problema a inclusão do seguinte parâmetro, no arquivo de configuração do samba "`smb.conf`", na seção "`[global]`":

  ```
  nt pipe support = no
  ```

- Após a mudança no arquivo, é necessário reiniciar o serviço "`smbd`".

Recomenda-se ainda, analise por parte da organização, para cada ativo de informação a necessidade da utilização do Samba. Caso não seja pertinente:

- Desativar o serviço "`smbd`";
- Bloquear as portas UDP 137, 138 e TCP 139, 445.

Referências:

- http://www.samba.org/samba/security/CVE-2017-7494.html
- https://access.redhat.com/security/cve/CVE-2017-7494

Brasília-DF, 25 de maio de 2017.

Equipe do CTIR Gov