Recomendação de Segurança 001/2022 - Cogetic

Em 2 de fevereiro de 2022

Para: Gestores de TI das unidades da Fiocruz

Assunto: Samba

Prezados Gestores de TI,

No dia 31 de janeiro de 2022 foi lançada uma correção para uma nova vulnerabilidade avaliada como crítica na solução Samba. A vulnerabilidade está detalhada na CVE-2021-44142 e possui classificação 9.9/10.0 no CVSS 3.0. A falha está presente em diversas versões de sistemas operacionais Linux, Solaris, e MacOS e pode permitir que um agente mal-intencionado realize uma execução de código remota com privilégios de root, obtendo acesso total ao sistema alvo.

As versões do Samba anteriores à 4.13.17 são consideradas vulneráveis ao "out-of-bounds read/write" (OBB), permitindo que invasores executem remotamente códigos com privilégio de root nas instalações Samba que usam o módulo "vfs_fruit" do sistema de arquivos virtual (VFS).

Conforme divulgado pelo Samba, "A falha específica existe na análise dos metadados do EA ao realizar a abertura de arquivos em SMBD. Para exploração da falha em questão, é necessário que um usuário (podendo ser guest ou não autenticado) possua acesso de gravação aos atributos estendidos do arquivo. O problema no "vfs_fruit" existe na configuração padrão do módulo Fruit VFS usando "fruit:metadata=netatalk" ou "fruit:resource=file". Se ambas as opções estiverem definidas com configurações diferentes dos valores padrão, o sistema não é afetado pelo problema de segurança."

Até o momento, a prova de conceito da vulnerabilidade não está disponível publicamente e não há relatos de tentativas de explorações massivas, contudo um invasor pode acionar essa vulnerabilidade sem interação do usuário.

Recomendações:

- Atualizar o Samba para uma versão mais recente e não vulnerável, disponível em: https://bugzilla.samba.org/show_bug.cgi?id=14914, ou diretamente da respectiva distribuição.

- Caso não seja possível uma atualização imediata, o Samba também fornece uma solução alternativa que consiste em remover o módulo VFS "fruit" da lista de objetos VFS configurados em qualquer linha de "vfs objects" no arquivo de configuração do Samba.

Referências

- https://www.samba.org/samba/security/CVE-2021-44142.html
- https://www.bleepingcomputer.com/news/security/samba-bug-can-let-remote-attackers-execute-code-as-root/
- https://securityaffairs.co/wordpress/127457/security/cve-2021-44142-samba-rce.html

Coordenação de Gestão de Tecnologia da Informação
Segurança da Informação e Comunicações