Ministério da Saúde

FIOCRUZ
Fundação Oswaldo Cruz

Recomendação de Segurança 003/2021 - Cogetic

Em 18 de maio de 2021

Para: Gestores de TI das unidades da Fiocruz

Assunto: Arquivos de controle acessíveis remotamente

Prezados,

Considerando o cenário atual de exposição da instituição e a necessidade de constante revisão e avaliação das infraestruturas críticas de TIC que suportam as atividades organizacionais e proveem serviços em geral à sociedade através da Internet, pedimos atenção das áreas de TI das unidades da Fiocruz para a exposição e acesso indevido de diretório e arquivos de configuração em servidores de aplicações web.

Alguns diretórios armazenados em servidores web podem conter arquivos sensíveis (geralmente relacionados à backup, configuração, autenticação, arquivos temporários etc.). Esses diretórios na maioria das vezes não estão diretamente vinculados à aplicação e, caso estejam indevidamente expostos, podem permitir a um usuário malicioso a obtenção de informações para a realização de ataques mais direcionados e eficientes.

Esse tipo de falha pode estar relacionada à diversas vulnerabilidades já identificadas e catalogadas em CWE's, tais como, CWE-200: *Information Exposure*, CWE-538: *File and Directory Information Exposure*, CWE-548: *Exposure of Information Through Directory Listing* etc.

Um exemplo dessa falha pode ocorrer na utilização ferramentas para versionamento de código (GitHub, por exemplo). Apesar de todos os benefícios trazidos por essas ferramentas, ao ser criado um diretório **/.git** no servidor em produção (que pode conter diversos arquivos, incluindo arquivos de configuração com informações sensíveis), caso o diretório não esteja adequadamente configurado, a exposição dos arquivos pode trazer grandes riscos à segurança. Outros exemplos são arquivos de configuração **.htaccess** no Apache, **web.config** no ISS, **.env** do Laravel, entre outros.

De uma forma geral, recomenda-se que diretórios que se iniciem com "." não tenham permissão para serem listados ou acessados externamente. Caso o seu conteúdo não seja necessário para o funcionamento da aplicação, o ideal é que seja removido do servidor web.

Uma das formas para correção do problema é especificar no arquivo de configuração do servidor web os diretórios/arquivos que precisam ter seu acesso restringido. Isso pode ser feito

utilizando expressões *regex* para restringir o acesso a arquivos iniciados com "**.**". Um exemplo dessas configurações pode ser encontrado no endereço https://gist.github.com/lynt-smitka/1ce5c4bb3a8d251df0b3268019787664. Contudo, a solução acima não é exaustiva e alternativas podem ser facilmente encontradas em fóruns na Internet.

Referências:

- CWE-200
  - https://cwe.mitre.org/data/definitions/200.html
- CWE-538
  - https://cwe.mitre.org/data/definitions/538.html
- CWE-548
  - https://cwe.mitre.org/data/definitions/548.html
- Como desabilitar o acesso a diretórios que começam com "**.**"
  - https://stackoverflow.com/questions/4352737/apache-configuration-regex-to-disable-access-to-files-directories-beginning-wit/16734602
- Tratamento do diretório /.git no Apache
  - https://stackoverflow.com/questions/38959525/hide-git-directory-or-file-with-apache
- Tratamento do diretório /.git no Nginx
  - https://gist.github.com/jaxbot/5748513
- Tratamento do diretório /.git no IIS
  - https://insights.ursinus.edu/display/LEI/Securing+GIT+folders+on+your+webserver

Coordenação de Gestão de Tecnologia da Informação

Segurança da Informação e Comunicações