CAIS-Alerta [22/02/2018]: Vulnerabilidades no CMS Drupal (CORE)

Prezados,

O CAIS alerta para as recentes vulnerabilidades encontradas no CMS Drupal que podem permitir acesso não autorizado a informações e exploração de vulnerabilidades do tipo Cross-Site-Script (XSS). Até o momento da publicação deste alerta, não foram identificados códigos de exploração para as vulnerabilidades identificadas.

Descrição

Vulnerabilidades existentes no Drupal 8

- - Formulário de resposta de comentários podem permitir acesso à conteúdos restritos:
Usuários com permissões para postar comentários podem visualizar conteúdos e comentários, bem como incluir outros comentários em conteúdos aos quais não lhes foi dado acesso;

- - Tratamento incorreto de acessos em sites multi-idiomas;
Em sites multi-idiomas com controle de acesso ativo, o Drupal aplica versões não traduzidas do ambiente como padrão para certas consultas. Dessa forma, em algumas situações, é possível que um conteúdo não permitido seja acessado devido a falta de tradução e uso da versão padrão do sistema.

- - Falha no controle de acesso ao módulo "Settings Tray" no Drupal 8:
O módulo "Settings Tray" possui uma vulnerabilidade que pode permitir aos usuários atualizar determinados tipos de informações sem ter permissão para tal ação;

Vulnerabilidades existentes no Drupal 7

- - Falha no controle de acesso de arquivos privados:
O Drupal possui verificação de restrições de acesso a arquivos antes que um usuário possa acessá-los, esta verificação pode falhar em certas circunstâncias onde um módulo tenta restringir o acesso enquanto outro permite acesso;

- - Vulnerabilidade do JQuery em domínios não-confiáveis:
Podem ocorrer circunstâncias de exploração de vulnerabilidade XSS no JQuery quando este faz requisições Ajax para domínios não-confiáveis;

- - Injeção de links externos em páginas apresentando o código de erro 404:
Quando o recurso de bloqueio baseado em idiomas está em uso, um usuário malicioso pode redirecionar usuários para uma página externa fraudulenta através dessa vulnerabilidade.

Vulnerabilidades existentes no Drupal 7 e 8

Prevenção contra Cross-Site-Script (XSS) via JavaScript insuficiente:
- - O Drupal possui uma função utilizada para sanitizar textos potencialmente perigosos antes de publicá-los, porém, esta função não gerencia corretamente todos os métodos de injeção de códigos maliciosos levando a exploração de vulnerabilidades XSS sob certas circunstâncias.

Sistemas impactados

Sistemas utilizando o Drupal 7.
Sistemas utilizando o Drupal 8.

Versões afetadas

Versão 7.56 e todas as versões anteriores subsequentes.

Versão 8.4.4 e todas as versões anteriores subsequentes.

Correções disponíveis

Atualizar a versão do CMS Drupal para a versão mais recente disponibilizada pelos desenvolvedores ou a versão mais recente recomendada de acordo com o sistema operacional em uso.

Identificadores CVE (http://cvw.mitre.org)

Não há.

Mais informações

https://www.drupal.org/sa-core-2018-001
https://www.us-cert.gov/ncas/current-activity/2018/02/21/Drupal-Releases-Security-Updates

O CAIS recomenda que os administradores mantenham seus sistemas e aplicativos sempre atualizados, de acordo com as últimas
versões e correções oferecidas pelos fabricantes.

Os alertas do CAIS também podem ser acompanhados pelas redes sociais da RNP.
Siga-nos!
Twitter: @RedeRNP
Facebook: facebook.com/RedeNacionaldeEnsinoePesquisaRNP.

###
CENTRO DE ATENDIMENTO A INCIDENTES DE SEGURANCA (CAIS)
Rede Nacional de Ensino e Pesquisa (RNP)
#   #
cais@cais.rnp.br   http://www.rnp.br/servicos/seguranca
Tel. 019-37873300   Fax. 019-37873301
Chave PGP disponivel   https://www.cais.rnp.br/cais-pgp.key
###

_____