Prezados,

O CAIS alerta para as recentes vulnerabilidades encontradas no CMS Drupal, que podem permitir execução arbitrária de código e possibilidade de burlar controles de acesso. Até o momento da publicação deste alerta, não foram identificados códigos de exploração para as vulnerabilidades identificadas.

DESCRIÇÃO

- Validação incorreta de controle de acesso via editor de textos(CVE-2017-6377)
Ao adicionar um arquivo via editor de texto (como o CKEditor), este não realiza a correta verificação dos arquivos anexados, o que pode permitir um atacante burlar o controle de acesso do ambiente.

- Inexistência de controles CSRF em alguns diretórios administrativos (CVE-2017-6379)
A falta de proteção contra ataques CSRF (Cross-Site Request Forgery) em alguns diretórios administrativos do Drupal pode permitir que um usuário malicioso execute comandos não autorizados através de um usuário autenticado, explorando a relação de confiança existente no ambiente. Caso o atacante tenha conhecimento dos IDs de blocos de um determinado site, estes podem ser desativados, por exemplo.

- Execução remota de código (CVE-2017-6381)
A biblioteca Composer, incluída dentre as dependências de desenvolvimento da versão 8 do Drupal, é vulnerável à execução remota de código.

VERSÕES AFETADAS
Versão 8.2.6 e todas as versões anteriores subsequentes.

CORREÇÕES DISPONÍVEIS
Atualizar a versão do CMS Drupal para a versão mais recente disponibilizada pelos desenvolvedores (8.2.7 no momento da publicação deste alerta) ou a versão mais recente recomendada de acordo com o sistema operacional em uso.

IDENTIFICADORES CVE (http://cve.mitre.org)
CVE-2017-6377,CVE-2017-6379
CVE-2017-6381

MAIS INFORMAÇÕES
https://www.drupal.org/SA-2017-001
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2017-6377
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2017-6379
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2017-6381
https://www.owasp.org/index.php/Cross-Site_Request_Forgery_(CSRF)
https://www.drupal.org/project/drupal/releases/8.2.7

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   http://www.rnp.br/cais/cais-pgp.key        #
#####################################################################
```