Presidência da República
Gabinete de Segurança Institucional
Departamento de Segurança da Informação e Comunicações
Centro de Tratamento de Incidentes de Segurança de Redes de Computadores da Administração Pública Federal

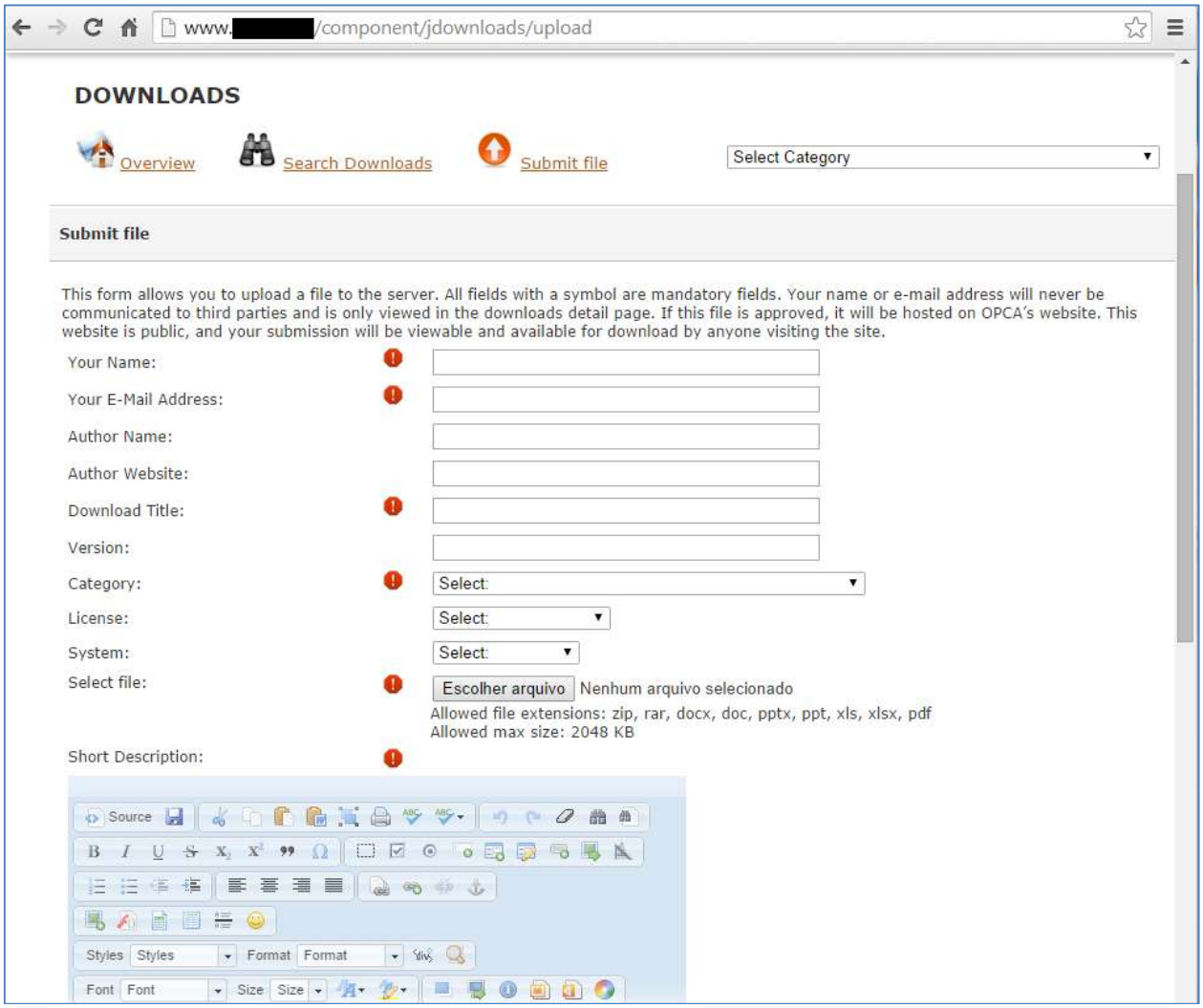
Alerta nº 06/2014 – JDownloads

1. Descrição do Problema

A extensão **JDownloads**, em algumas versões ainda não identificadas, utilizado em sítios desenvolvidos com o Gerenciador de Conteúdo **Joomla!**, permite que um usuário não autorizado insira arquivos no servidor, por meio de uma interface de inclusão de arquivos, que pode ser acessada por URLs do tipo:

- http://<*dominio*>/component/jdownloads/upload/

Como por exemplo:



Ou ainda podem ser encontradas em buscas na internet com consultas do tipo, para o Google:

submit file author inurl:upload site:<*domínio de interesse*>

Após a inserção, o arquivo pode ser acessado em URLs do tipo:

- http://<*dominio*>/images/jdownloads/screenshots/<*nome_arquivo*>

Os arquivos que foram inseridos nos servidores, que identificamos até o momento, são apenas figuras com menções a desfigurações dos sítios. Porém é provável que outros arquivos possam ser inseridos no servidor, como *malwares* e *shells*, que podem comprometer inteiramente o servidor e até mesmo a rede interna.

2. Possíveis Riscos

Comprometimento do servidor;

Comprometimento da rede de servidores;

Comprometimento do banco de dados do sítio;

Hospedagem de malwares;

Uso indiscriminado do servidor, como por exemplo, para outros ataques.

3. Sugestões para Mitigação do Problema

Aparentemente o problema foi solucionado pelo desenvolvedor da extensão JDownloads, como pode ser observado no fórum da extensão, como por exemplo em:

- http://www.jdownloads.com/forum/index.php?topic=7336.msg28498
- http://www.jdownloads.com/forum/index.php?topic=7326.msg28493

Portanto sugerimos a **atualização** da extensão para a última versão estável disponibilizada pelo desenvolvedor, que pode ser encontrada em:

- http://www.jdownloads.com/index.php?option=com_jdownloads&view=viewcategories&Itemid=133

Sugerimos que seja restringido o permissionamento das pastas e dos arquivos do sítio, seguindo a orientação do desenvolvedor, tanto da extensão, quanto do Gerenciador de Conteúdo Joomla!, que pode ser encontrado em:

- http://docs.joomla.org/Security_Checklist/Joomla!_Setup

Referências:

- http://www.youtube.com/watch?v=78VDikFvLl8
- http://www.jdownloads.com/forum/index.php?topic=7336.msg28498
- http://www.jdownloads.com/forum/index.php?topic=7326.msg28493
- http://docs.joomla.org/Security_Checklist/Joomla!_Setup

Brasília-DF, 12 de Setembro de 2014

Atenciosamente,

Equipe do CTIR Gov