

CAIS-Alerta: vulnerabilidade no plugin PHP Weathermap para CACTI

[RNP, 08.11.2013-, revisão 01]

O CAIS recebeu uma notificação sobre uma vulnerabilidade presente na instalação/configuração do plugin PHP Weathermap para o CACTI.

A vulnerabilidade existe na configuração padrão do PHP Weathermap, o qual não restringe corretamente o acesso ao arquivo de configuração dos mapas. Um atacante remoto, sem acesso as configurações do Weathermap, poderia editar e/ou apagar os mapas de redes previamente cadastrados.

CORREÇÕES DISPONÍVEIS

Recomenda-se aplicar ao menos uma das correções listadas abaixo:

1- Limitar os usuários que podem acessar o editor de mapas via Apache (Diretiva FilesMatch):

```
<Directory /var/www/html/cacti/plugins/weathermap> "Diretório padrão de instalação"  
<Files editor.php>  
Order Deny,Allow  
Deny from all  
Allow from 127.0.0.1 "Trocar pelo ip da rede autorizada"  
</FilesMatch>  
</Directory>
```

Mais informações em:

<http://www.network-weathermap.com/manual/0.97b/pages/install-cacti-editor.html>

2 - Limitar os usuários que podem acessar o editor de mapas via Apache (Diretiva htaccess) - **Recomendação:

<http://httpd.apache.org/docs/current/howto/htaccess.html>

<http://www.thesitewizard.com/apache/password-protect-directory.shtml>

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 são oferecidos no formato RSS/RDF e no Twitter:

<http://www.rnp.br/cais/alertas/rss.xml>

Siga @caismp.