

# INTRUDERS TIGER TEAM SECURITY SECURITY ADVISORE

<http://www.intruders.org.br>  
<http://www.intruders.com.br>

ADVISORE 01/07 - UEBIMIAU INSECURE HANDLE PASSWORDS

PRIORIDADE: BAIXA

I - INTRODUÇÃO:

-----

De <http://www.uebimiau.org/>

**“Uebimiau is an universal webmail developed in PHP by Aldoir Ventura. It is free and can be installed in any email server.”**

Tradução livre:

“UebiMiau é um webmail universal desenvolvido em PHP por Aldoir Ventura. Ele é livre e pode ser instalado em qualquer servidor de email.”

II - DESCRIÇÃO:

-----

Durante um Pen-test, a equipe do Intruders Tiger Team Security tem identificado uma vulnerabilidade no Uebimiau Webmail Server em sua instalação padrão que pode ser explorada por usuários maliciosos locais para obter passwords de email validos em modo limpo(sem nenhuma criptografia).

Intruders Tiger Team Security tem descoberto que muitos sistemas se encontram

vulneráveis.

### III - ANÁLISE

Uebimiau em sua instalação padrão, cria um arquivo de sessão para armazenar dados de conexão com servidores pop, imap em modo limpo. Quem gerencia a criação desse arquivo é o próprio php no webserver e não raro se encontra no diretório /tmp.

Se um atacante tem acesso local ao webserver onde se encontra o UEBIMIAU, ele poderia então “ler” esses arquivos de sessão e capturar senhas de outros usuários em “modo limpo”.

Abaixo, podemos visualizar um exemplo real desse problema.

```
$ cat /tmp/sess_866b59f58716f0fd33559d0d1620f6cb
```

```
um_session_data|
a:15:{s:5:"start";i:1191553448;s:5:"email";s:18:"nashleon@localhost";s:4:"user";s:8:
"nashleon";s:4:"pass";s:12:"senha_aqui!";s:6:"server";s:9:"localhost";s:4:"port";i:1
10;s:8:"protocol";s:4:"pop3";s:13:"folder_prefix";s:0:"";s:9:"remote_ip";s:9:"127.0.
0.1";s:7:"headers";a:1:{s:8:"aW5ib3g=";a:6:{i:0;a:17:{s:2:"id";i:6;s:3:"msg";s:1:"6"
;s:4:"size";s:3:"830";s:6:"header";s:751:"Return-Path: <nobody@inspiron.localdomain>
```

Note alguns valores desse arquivo:

email == [nashleon@localhost](mailto:nashleon@localhost)

user == nashleon

pass == senha\_aqui!

server == localhost

port == 110

protocol == pop3

remote\_ip == 127.0.0.1

Como podemos analisar, trata-se de informações de acesso a uma conta POP num determinado servidor pop (no caso descrito acima, o servidor pop é local).

O agravante desse problema é a senha em modo limpo. Um atacante com

acesso web local poderia carregar scripts para ler esses arquivos de sessao e capturar as senhas de outros usuarios, e isso eh preocupante em sistemas de WEB Hosting.

#### IV. DETECÇÃO

-----

A Equipe do Intruders Tiger Team Security tem confirmado a existência dessa vulnerabilidade no UebiMiau versão 2.7.10.

Outras versões possivelmente podem estar vulneráveis também.

#### V. WORKAROUND

-----

Recomendamos executar o UEBIMIAU em uma maquina isolada(talvez VMWARE). Nenhum sistema de protecao presente no PHP eh confiavel.

#### VI - CRONOLOGIA

-----

21/07/2007 - Falha descoberta durante um Pen-Test.

05/10/2007 - Uebimiau Team Contatado.

??/10/2007 - Resposta do Fabricante.

??/10/2007 - Advimore publicado.

#### VII - CREDITOS

-----

Glaudson Ocampos(Nash Leon) e Intruders Tiger Team Security tem descoberto esta vulnerabilidade.

Agradecimentos a Wendel Guglielmetti Henrique (dum\_dum), Ygor da Rocha Parreira(dmr), Waldemar Nehgme (mastermind) e Elio da Security OpenSource.

Visite o Web Site do Intruders Tiger Team Security para ver outros adviores:

<http://www.intruders.com.br/>

<http://www.intruders.org.br/>

