

VulnWatch: [VulnWatch] Digi-news and Digi-ads version 1.1 admin access without password

[VulnWatch] Digi-news and Digi-ads version 1.1 admin access without password

Source: <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2003-07/0031.html>

From: scrap (webmaster_at_securiteinfo.com)

Date: 07/16/03

To: bugtraq@securityfocus.com, full-disclosure@lists.netsys.com

Date: Wed, 16 Jul 2003 20:18:23 +0200

Digi-news and Digi-ads version 1.1 admin access without password

.oO Overview Oo.

Digi-news and Digi-ads version 1.1 admin access without password

Discovered on 2003, March, 30th

Vendor: Digi-FX

Digi-news 1.1 is a PHP news editor. It allows you to easily add, edit, and delete news.

Digi-ad 1.1 is a PHP ad rotator. It allows you to easily add, edit, reset, and delete ads.

A vulnerability allows to access to the admin area in both script, without the administrator password.

Original text is at

http://www.securiteinfo.com/attaques/hacking/digi-news1_1.shtml

.oO Details Oo.

In Digi-news or Digi-ad, the admin web page is admin.php

Here is a sample of the admin authentication in this admin.php :

```
if (!isset($action)) {
    $action = "";
}
if ($action == 'auth') {
    auth();
}
if ((@$HTTP_COOKIE_VARS['user'] != $digiNews['user']) &&
(@$HTTP_COOKIE_VARS['pass'] != md5($digiNews['pass']))) {
    login();
    exit;
}
```

Continued as admin logged...

As you can see, the authentication scheme is based on a cookie. This cookie contains the user and the MD5 hashed password. But the programmer did a

VulnWatch: [VulnWatch] Digi-news and Digi-ads version 1.1 admin access without password

mistake :

```
if ((@$HTTP_COOKIE_VARS['user'] != $digiNews['user']) &&  
(@$HTTP_COOKIE_VARS['pass'] != md5($digiNews['pass']))) {
```

It means that "Admin is authenticated" if "user = user in the cookie" OR "password = password in the cookie". In english, it means you don't need the admin password as far as you know the admin login !

The default admin login is "admin". If it doesn't work, try these :

- * Admin
- * Administrator
- * administrator
- * Root
- * root
- * the nickname of the admin (if known)
- * the surname of the admin (if known)
- * etc...

.oO Exploit Oo.

Ok, that's quite easy. You just have to send a handwritten cookie with user=admin in. You can do that with the well-known Proxomitron

.oO Solution Oo.

The solution is to replace the AND operation by a OR operation, as followed :

```
if ((@$HTTP_COOKIE_VARS['user'] != $digiNews['user']) ||  
(@$HTTP_COOKIE_VARS['pass'] != md5($digiNews['pass']))) {
```

The vendor has been informed and solved the problems. Download Digi-News 1.2 and Digi-ads 1.2 at <http://www.digi-fx.net/freescripts.php>

.oO Discovered by Oo.

Arnaud Jacques aka scrap
webmaster@securiteinfo.com
<http://www.securiteinfo.com>