

[NT] Multiple Vulnerabilities in ASPapp Products

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-12/0067.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 12/22/03

To: list@securiteam.com

Date: 22 Dec 2003 12:50:33 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

Multiple Vulnerabilities in ASPapp Products

SUMMARY

<<http://www.aspapp.com>> ASPapp is "a complete, easy-to-modify .asp portal system. With this portal, you can manage users, content, links, files, forums, surveys, product catalog, shopping cart, PayPal or Authorize.net e-commerce, classifieds, calendar, download images, surveys, FAQ's, news, and more. Currently it is one of the most popular. The vulnerabilities listed below affect IntranetApp and ProjectApp, as the codebase is almost identical". The products contain multiple security vulnerabilities privilege escalation, account hijacking, cross-site scripting, code injection, and plaintext password storage.

DETAILS

Privilege Escalation Vulnerability:

This vulnerability allows a malicious user set himself any user level he desires. This is because the user level is determined by a hidden form field value titled "accesslevel". If a user sets it to the "Super Admin" level (level number 4), they can pretty much take over the entire portal.

They can also view other user's passwords in plaintext via the "User Admin" feature by viewing the HTML source. This does vulnerability is not present in IntranetApp, but it is present in PortalApp and ProjectApp.

Securiteam: [NT] Multiple Vulnerabilities in ASPApp Products

Account Hijacking Vulnerability:

Once again, ASP App software relies on hidden form fields to determine user values. By changing the "user_id" field, a malicious user can reset passwords for arbitrary accounts and edit their user information. This is vulnerability present in all three applications.

Cross Site Scripting Vulnerabilities:

XSS is possible on any page of an ASP APP Portal by appending the variable "msg" with a value of any script you would like to be run. For example the following. `default.asp?msg=%3Ciframe%3E` this vulnerability also exists in all 3 applications.

Code Injection Vulnerabilities:

There are a number of places you can inject code and have it run by a user or an administrator. This includes but not limited to the following.

An injection vulnerability exists in `forums.asp`. When posting a new message, a script can be injected into the Title and into the message form fields. This is especially dangerous as the latest message is posted on the main page of the website, therefore affecting all users.

An injection vulnerability exists in `submit.asp`. A malicious user can submit script instead of a link to be added to the website. This vulnerability affects the administrator when he prepares to accept or deny submissions.

An injection vulnerability is present in the profile section of the website. By submitting a script into the fields of `upd_user.asp` (the profile update form), an attacker can cause it to run whenever someone views the affected profile (`user_public.asp`). The form fields that are vulnerable are First Name, Last Name and Country. This vulnerability exists in all three of the previously mentioned ASP APP scripts.

Plaintext Password Storage Weakness:

The username and password are stored as plaintext inside a cookie, making cookie theft through a cross-site scripting vulnerability more dangerous. This vulnerability exists in all three of the previously mentioned ASP APP scripts.

Solution:

The vendor plans on releasing a new version of these products at the end of the month to supposedly correct all of the security issues mentioned above.

ADDITIONAL INFORMATION

The information has been provided by security@gulftech.org
JeiAr.

=====

Securiteam: [NT] Multiple Vulnerabilities in ASPapp Products

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====
=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.