

# [NT] Facto System CMS Contains Multiple Vulnerabilities

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-08/0120.html>

---

*From:* [support@securiteam.com](mailto:support@securiteam.com)

*Date:* 08/31/02

From: [support@securiteam.com](mailto:support@securiteam.com)

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: Sat, 31 Aug 2002 09:15:53 +0200 (CEST)

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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

-----

Facto System CMS Contains Multiple Vulnerabilities

---

## SUMMARY

<<http://sourceforge.net/projects/facto>> Facto is a collaborative, dynamic Web publishing system. The system can be used for creating personal or group 'Blog' type sites. It is written entirely in Active Server Pages (ASP) and can use Microsoft Access or SQL Server as a database backend. The product has been found to contain multiple security vulnerabilities allowing a remote attacker to insert into existing SQL queries arbitrary SQL statements.

## DETAILS

Vulnerable systems:

- \* IIS 4.0 or later with ASP enabled and Facto System CMS installed

Multiple SQL injection vulnerabilities exist in the Facto System Content Management System that may allow an attacker to introduce instructions into an SQL query. The vulnerabilities exist because the script fails to verify the validity of numeric data and fails to properly escape certain control characters in strings.

## Securiteam: [NT] Facto System CMS Contains Multiple Vulnerabilities

The problems are in the handling of the query variables "authornumber" (in author.asp), and "discussblurbid" (in discuss.asp), and the form variables "name" and "email" (in holdcomment.asp).

Example:

An example is below:

```
http://localhost/author.asp?authornumber=1%28%20And%20AuthorTable%2EAuthorID%3DBlurbTable%2EAuthorID%20And%20BlurbTable%2ESub_id%3DSubjectTable%2ESub_id%20Order%20By%20BlurbTable%2EBlurbdate%20desc%2C%20blurbtable%2Eblurbtime%20desc%3BUPDATE%20user%20SET%20Password%3DPASSWORD%28%27password%27%29%20WHERE%20user%3D%27root%27%3B%20FLUSH%20PRIVILEGES%3B---
```

### ADDITIONAL INFORMATION

The information has been provided by <mailto:[mattmurphy@kc.rr.com](mailto:mattmurphy@kc.rr.com)>  
Matthew Murphy.

=====

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](mailto:list-unsubscribe@securiteam.com)

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

- 
- **Previous message:** [support@securiteam.com](mailto:support@securiteam.com): "[EXPL] GDAM123 Exploit Code Released"
  - **Messages sorted by:** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)