

# [NEWS] Vignette /vgn/legacy/save SQL Access

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-05/0070.html>

---

**From:** SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

**Date:** 05/31/03

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

Date: 31 May 2003 11:03:04 +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

In the US?

Contact Beyond Security at our new California office housewarming rates on automated network vulnerability scanning. We also welcome ISPs and other resellers!

Please contact us at: 323-882-8286 or [ussales@beyondsecurity.com](mailto:ussales@beyondsecurity.com)

-----

Vignette /vgn/legacy/save SQL Access

---

## SUMMARY

<<http://www.vignette.com/>> Vignette develops Content Management and Application Portal Software. A sample application that comes with the server allows complete access to the Vignette's underlying SQL server.

## DETAILS

Vulnerable systems:

- \* Vignette StoryServer 4, StoryServer 5 and Vignette V/5.

Vignette Software installs by default some helper applications under the /vgn web directory.

One of these applications is the Vignette Legacy Tool. This application is usually accessed through it's main template /vgn/legacy/edit. This template is protected by the [ NEEDS LOGIN ] directive and it's not accessible for unauthenticated users.

The problem is that the processing backbone of this application is carried by the /vgn/legacy/save template, which is not protected by the [ NEEDS

Securiteam: [NEWS] Vignette /vgn/legacy/save SQL Access

LOGIN ], but it rather only uses the RECORD directive. However, this check is easily bypassed, as the check only looks for a vgn\_creds cookie (without checking its content). Meaning that we only needed to place some random value in the cookie to do a successful query.

Solution:

Insert a [ NEEDS LOGIN ] directive in the top of the source code for the /vgn/legacy/save template. Vignette users should proceed to contact vignette through the standard channels VOLS etc in order to get a solution.

ADDITIONAL INFORMATION

The original advisory can be downloaded from:

<<http://www.s21sec.com/es/avisos/s21sec-017-en.txt>>  
<http://www.s21sec.com/es/avisos/s21sec-017-en.txt>

The information has been provided by <mailto:vul-serv@s21sec.com> S21SEC.

=====

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.