

Securiteam: [NEWS] Vignette Story Server Sensitive Information Disclosure

# [NEWS] Vignette Story Server Sensitive Information Disclosure

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-04/0032.html>

---

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

*Date:* 04/18/03

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

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

Date: 18 Apr 2003 13:12:52 +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 Story Server Sensitive Information Disclosure

---

## SUMMARY

Vignette's Story Server is a web interface to Vignette's content management suite of applications that operates on a variety of platforms and web server technologies.

Vignette Story Server allows the publication of both static and dynamic content. The dynamic pages are created using a TCL[1] Interpreter. There exists vulnerability within the TCL interpreter used that allows 'dumping' of the stack of the current running TCL process when generating dynamic pages.

This vulnerability results in an attacker being able to extract information about other users sessions, server side code and other sensitive information.

This vulnerability has been verified on Vignette Story Server v4.1 and v6.0.

## DETAILS

Vulnerable systems:

- \* Vignette Story Server version 4.1
- \* Vignette Story Server version 6

Vignette supports a vast range of dynamic content via its content management system. It allows the use of TCL code to interact with databases, generate cookies, and wide range of other functions.

When a request is made to a dynamic page which accepts user input there exists an issue when a large number of " and > characters are input to the TCL interpreter. The effect is that the TCL interpreter will crash returning to the user the data that was on the stack at the current time.

– From @stake's testing it has been observed the most likely way to generate the crash is with a combination of around 214 " and > characters. Contained below is an example URL that if populated would return a large amount of data.

[https://www.example.co.uk/securelogin/1.2345.A.00.html?Errmessage="x214>x214](https://www.example.co.uk/securelogin/1.2345.A.00.html?Errmessage=) [line wrapped]

If above URL is submitted when there is a large number of users performing dynamic functions within the site (i.e. logging in or performing a search) then a large amount of sensitive TCL code will be available upon the stack and send to the attacker.

It should be noted that this vulnerability can be exploited continuously without any effect on the availability of the site in question, thus allowing an attacker to effectively wait until they have enough data to achieve their end goal.

Timeline:

Jan. 28, 2003 Email contact at Vignette on 28th with details of vulnerability. Received questions regarding vulnerability and respond accordingly.

February 2003 Vignette confirms they have not been able to reproduce @stake calls Vignette contact to explain vulnerability, understand the product is not affected in its latest incarnation due to it being Java rather than TCL. Contact says they would like affected customers to upgrade. @stake offers via voice and e-mail to reproduce issue if Vignette provide Internet accessible host. @stake conducts another phone call with Vignette to explain the issue and discuss possible alternatives and solutions @stake has been suggesting to clients.

March 2003 @stake contact Vignette requesting an update. Vignette states that questions regarding this issue should be submitted by affected customers via their Vignette support contract.

Securiteam: [NEWS] Vignette Story Server Sensitive Information Disclosure

April 4, 2002 Vignette responds that the issue has been fixed and supplies patch information.

\* It should be noted that @stake customers were affected by this issue and our first priority was to not put them at increased risk.

Vendor Response:

The problem is fixed and a patch is available. Any Vignette customer who has a security concern with their Vignette deployment should contact Vignette Technical Support through normal channels. Those channels include <mailto:support@vignette.com> support@vignette.com, contacting Technical Support in the Americas at 1 888 846 6907, Europe, Middle East and Africa 44(0)1628772299 and Asia Pacific Australia 1 800 110 118 Asia Pacific New Zealand, Singapore, Hong Kong, Taiwan & China: +800 110 11811 Asia Pacific All Others 61.2.9455.5099. Additionally, customers have the following resources available at

<http://support.vignette.com/VOLSS/KB/View/1,,5360.00.html>  
http://support.vignette.com/VOLSS/KB/View/1,,5360.00.html and  
<http://support.vignette.com/VOLSS/KB/View/1,,5360.00.html>  
http://support.vignette.com/VOLSS/KB/View/1,,5360.00.html

@stake Recommendations:

If you have a dynamic application that receives user input you should install the patch.

Alternatively, employ string length checks upon user submitted data. @stake has discovered requests under about 100 bytes rarely yield any sensitive information.

ADDITIONAL INFORMATION

The information has been provided by <mailto:ollie@atstake.com> Ollie Whitehouse of @Stake.

=====

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.