

## **NISCC Vulnerability Advisory 260146/NISCC/SITESCAPE**

### **Vulnerability Issues with SiteScape Forum**

#### **Version Information**

Advisory Reference	260146/NISCC/SITESCAPE
Release Date	25 May 2006
Last Revision	25 May 2006
Version Number	1.0

#### **Acknowledgement**

These vulnerabilities were reported to NISCC by ProCheckup Ltd (<http://www.procheckup.com>).

#### **What is Affected?**

The following products are affected:

- SiteScape Forum v7.2 and possibly earlier

#### **Impact**

If these vulnerabilities were exploited, they could lead to unintentional information disclosure that can be used in other forms of attacks.

#### **Severity**

This is rated as low.

#### **Summary**

SiteScape Forum is a collaboration, workflow and messaging application. Two vulnerabilities have been identified by ProCheckup Ltd that can lead to unintentional information disclosure by the software.

1. Server webroot disclosure
2. Enumeration of valid usernames

The vendor, SiteScape, is aware of these issues and has produced patches to address the problems. Please see 'Solution' for details on patches required to address these flaws.

## **Details**

*260146/NISCC/SITESCAPE/1*

*CVE ID: NA*

The SiteScape Forum configuration file, avf.rc, discloses the server's webroot. If exploited, this can lead to information being disclosed that may be valuable to a malicious person.

*260146/NISCC/SITESCAPE/2*

*CVE ID: NA*

The SiteScape Forum program, dispatch.cgi/\_user/userCard/, allows the enumeration of valid usernames through differing responses to requests.

The successful enumeration of valid usernames may allow a malicious person to target password attacks against known user accounts.

## **Mitigation**

To minimise the risk of these vulnerabilities being exploited, please ensure that the forum is not available externally outside of your organisation.

## **Solution**

Please contact SiteScape to obtain the necessary patches.

## **Vendor Information**

SiteScape, Inc. offers scalable solutions for collaboration and knowledge management. SiteScape software is built on a platform-independent, web-based architecture and is used worldwide. For more information about SiteScape, visit <http://www.sitescape.com>.

## **Acknowledgements**

The NISCC Vulnerability Management Team would like to thank ProCheckUp Ltd for discovering and reporting these issues to

NISCC. For more information regarding ProCheckup Ltd, please visit <http://www.procheckup.com>.

The NISCC Vulnerability Management Team would also like to thank SiteScape for their co-operation in the handling of these vulnerabilities.

### Contact Information

The NISCC Vulnerability Management Team can be contacted as follows:

Email	<a href="mailto:vulteam@nisc.gov.uk">vulteam@nisc.gov.uk</a> <i>(Please quote the advisory reference in the subject line.)</i>
Telephone	+44 (0)870 487 0748 Extension 4511 <i>(Monday to Friday 08:30 - 17:00)</i>
Fax	+44 (0)870 487 0749
Post	Vulnerability Management Team NISCC PO Box 832 London SW1P 1BG

We encourage those who wish to communicate via email to make use of our PGP key. This is available from <http://www.nisc.gov.uk/nisc/publicKey2-en.pop>.

Please note that UK government protectively marked material should not be sent to the email address above.

If you wish to be added to our email distribution list, please email your request to [uniras@nisc.gov.uk](mailto:uniras@nisc.gov.uk).

### What is NISCC?

For further information regarding the UK National Infrastructure Security Co-Ordination Centre, please visit the NISCC web site at: <http://www.nisc.gov.uk/>

Reference to any specific commercial product, process or service by trade name, trademark manufacturer or otherwise, does not constitute or imply its endorsement, recommendation, or favouring by NISCC. The views and opinions of authors expressed within this

notice shall not be used for advertising or product endorsement purposes.

Neither shall NISCC accept responsibility for any errors or omissions contained within this advisory. In particular, they shall not be liable for any loss or damage whatsoever, arising from or in connection with the usage of information contained within this notice.

© 2006 Crown Copyright

### **Revision History**

25 May 2006      Initial release (1.0)

<End of NISCC Vulnerability Advisory>