

## **NISCC Vulnerability Advisory 356752/NISCC/MINDALIGN**

### **Several Vulnerability Issues Affecting the MindAlign Product**

#### **Version Information**

Advisory Reference	356752/NISCC/MINDALIGN
Release Date	12 August 2005
Last Revision	12 August 2005
Version Number	1.0

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

The following versions of the product are affected:

- MindAlign v5.0 and later

#### **Impact**

If exploited, these vulnerabilities could cause a variety of outcome; these can include denial-of-service, information disclosure and the ability for malicious people to obtain valid login credentials from the system.

#### **Severity**

This will vary by vulnerability; depending on which vulnerability is exploited, the severity can range from low to high.

#### **Summary**

Several vulnerabilities have been identified within the MindAlign product; these vulnerabilities ranges from bad configuration parameters to out-of-date third-party software relied upon by MindAlign.

Parlano have addressed the problems and have solutions available to rectify the flaw. Please see the 'Solution' section for further details.

## **Details**

Parlano's MindAlign is a Java (J2EE) application built on messaging services; as such, MindAlign has the standard IM and chat capabilities and also brings to the mix the ability to maintain persistent forums, chat threads, and other forms of group communication not found in ordinary IM (Instant Messaging) systems.

Several vulnerabilities have been discovered within the MindAlign product, although some are related to third-party products relied upon by MindAlign. There are varying vulnerabilities including 'User Enumeration', 'Cross-Site Scripting (XSS)', 'Bypassing Authentication' and 'Weak Encryption'.

As a result of exploiting these vulnerabilities, the outcomes can include 'Denial-of-Service', 'Information Disclosure' and 'Unauthorised Access'.

## **Mitigation**

Parlano has addressed the discovered vulnerabilities in bug-fix versions for their 5.x products and later. Please contact Parlano support at support@parlano.com for an upgrade.

## **Solution**

Subsequent versions of the product have addressed vulnerabilities identified in this report.

## **Vendor Information**

Parlano, Inc. is a leading provider of intelligent enterprise instant messaging solutions. The company is based in Chicago, IL with international headquarters London, England. For further details regarding Parlano, please visit their website at <http://www.parlano.com> or call +1.312/655.8330 or +44.207.743.6480.

## **Credits**

The NISCC Vulnerability Team would like to thank Parlano for their co-operation in the handling of this issue.

## **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.

## **Revision History**

12 August 2005 Initial release (1.0)

<End of NISCC Vulnerability Advisory>