

## Vulnerability Advisory

<b>Name</b>	Muster Render Farm Management System Arbitrary File Download
<b>Vendor Website</b>	<a href="http://www.vvertex.com/muster.html">http://www.vvertex.com/muster.html</a>
<b>Date Released</b>	November 29, 2011
<b>Affected Software</b>	Muster < 6.20
<b>Researcher</b>	Nick Freeman (nick.freeman@security-assessment.com)

### Description

Security-Assessment.com has discovered a vulnerability with the Muster 6.1.6 web management server. This issue can be exploited by an unauthenticated user to gain full control of the web management interface, and to send arbitrary commands to all Muster clients.

### Exploitation

It is possible to download any file on the Muster server by exploiting a vulnerability in the web server. By using directory traversal characters (\\.\..) in the URL, it is possible to specify any file on the file system to be served to the client. Exploitation of this vulnerability does not require authentication. The table below includes an example HTTP Request that would allow the download of the "muster.db" SQLite database:

#### Example of Malicious HTTP Request

```
GET /a\..\..\muster.db HTTP/1.1  
Host: musterserver:8690
```

This SQLite database contains a table with all users of the application together with base64-encoded passwords. By retrieving this database or other similar configuration files, it is possible to gain administrative access over the render farm.

### Solution

A patch is available from the vendor's website. Version 6.20 remediates this vulnerability.

### About Security-Assessment.com

Security-Assessment.com is Australasia's leading team of Information Security consultants specialising in providing high quality Information Security services to clients throughout the Asia Pacific region. Our clients include some of the largest globally recognised companies in areas such as finance, telecommunications, broadcasting, legal and government. Our aim is to provide the very best independent advice and a high level of technical expertise while creating long and lasting professional relationships with our clients.

Security-Assessment.com is committed to security research and development, and its team continues to identify and responsibly publish vulnerabilities in public and private software vendor's products. Members of the Security-Assessment.com R&D team are globally recognised through their release of whitepapers and presentations related to new security research.