Stoneware Security Bulletin
September 12, 2012

Summary
This security bulletin is provided to notify customers of security vulnerabilities within the webNetwork product. Stoneware has released webNetwork 6.1 Service Pack 1 to address these issues. The vulnerabilities could allow for unintended information disclosure and breach of user accounts. The impact of exploitation of these vulnerabilities depends on the sensitivity of the content contained within webNetwork. This vulnerability can allow for arbitrary execution of supplied JavaScript, which could be used to exploit vulnerabilities within a web browser, such as malicious code execution.

Vulnerability Information

<table>
<thead>
<tr>
<th>ID</th>
<th>Description</th>
<th>Maximum Security Impact</th>
<th>Severity Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2012-4352</td>
<td>Users vulnerable to cross-site scripting (XSS)</td>
<td>Information Disclosure / Breach of user account</td>
<td>Important</td>
</tr>
</tbody>
</table>

Recommendation
Stoneware recommends that customers upgrade to webNetwork 6.1 Service Pack 1 at the earliest opportunity.

Acknowledgements
Stoneware would like to thank Jacob Holcomb of Leland Public Schools for reporting CVE-2012-4352.

Disclaimer
The information provided by Stoneware in this bulletin and in the Stoneware Knowledge Base is provided "as is" without warranty of any kind. Stoneware disclaims all warranties, either express or implied, including the warranties of merchantability and fitness for a particular purpose. In no event shall Stoneware, Inc. or its suppliers be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages, even if Stoneware, Inc. or its suppliers have been advised of the possibility of such damages. Some states do not allow the exclusion or limitation of liability for consequential or incidental damages so the foregoing limitation may not apply.

Revisions
1.0, 2012-September-12, Bulletin published.