Livelink UTF-7 XSS Vulnerability

Release date: 31/Jan/2008
Last Modified: N/A
Author: David Kierznowski http://withdk.com
Application: Linklink <= 9.7.0
Risk: Medium

Quote from: http://www.opentext.com:
"Livelink features several advanced foundational elements that allow organizations to rapidly and easily enable advanced content management applications and solutions throughout the enterprise."

Livelink fails to auto-set the charset in the HTTP response header or in the HTML body. This means it is possible to trick several browsers into decoding Livelink pages in UTF-7. This allows attackers to inject arbitrary UTF-7 JavaScript into dynamic content that is echoed back to the user's browser.

Proof of concept:
None disclosed.

Disclosure information:

18/Jan/2008: Disclosed to vendor
25/Jan/2008: New version will auto-select UTF-8 encoding if one is not used.
31/Jan/2008: Advisory released

Affected versions:

9.0.0 Affected
9.1.0 Affected
9.2.0 Affected (Not tested)
9.5.0 Affected
9.6.0 Affected (Not tested)
9.7.0 Affected (Not tested)

Note: All versions without an encoding configured are vulnerable.

References: N/A