

Security Bulletin

For

Consona Live Assistance

Consona Dynamic Agent

Consona Subscriber Assistance

April 16, 2010

© 2010 Consona CRM Inc. All Rights Reserved. DNA®, DNAProbe®, HomeNet®, LiveAssist®, SmartAccess®, SmartIssue®, SmartResult®, SupportAction®, SupportSoft®, and SupportTrigger® are registered trademarks of the Consona companies. All product and company names should be considered trademarks of their respective companies and organizations.

Consona CRM Inc. makes no representations or warranties of any kind with respect to the contents of this document. Consona CRM Inc. shall not be held liable for errors contained herein or for incidental or consequential damage in connection with its use. Consona CRM Inc. reserves the right to revise this document and to make changes in its content without obligation to notify anyone of such revisions or changes.

Consona Live Assistance, Consona Dynamic Agent, and Consona Subscriber Assistance are covered by one or more of the following patents. U.S. Patent Nos. 5,996,073; 6,158,001; 6,163,859; 6,167,358; 6,266,788; 6,442,684; 6,754,707; 7,010,693 and 7,610,575. Other Patents Pending.

Security Vulnerabilities and Recommendations

Overview

This document outlines security updates for Consona Live Assistance, Consona Dynamic Agent, and Consona Subscriber Assistance. We recommend that you install all security updates as soon as they become available.

We take the security of our products very seriously and therefore do not disclose, discuss, or confirm security issues until we thoroughly investigate them and until any necessary patches or releases are available.

Security Issues

The following table describes several known security issues and our recommendations for resolving them.

1	<p>Problem Anonymous users can reset the Consona (<i>SupportSoft</i>) user password.</p> <p>Description If both the Hint question and the answer are blank in the “Forgot Password” page, an anonymous user can successfully reset a password with the blank question and the answer.</p> <p>Impact Rating Critical</p> <p>Recommendation Do not allow users who use a blank Hint question and answer to reset their password. Apply patch 1376 through Expert Exchange.</p> <p>Affected Products Consona Live Assistance Consona Dynamic Agent Consona Subscriber Assistance</p>
2	<p>Problem Consona (<i>SupportSoft</i>) Web servers are vulnerable to XSS.</p> <p>Description Some ASP pages on the Consona (<i>SupportSoft</i>) Web server are vulnerable to cross-site scripting attacks.</p> <p>Impact Rating Critical</p> <p>Recommendation Properly encode all parameters that are passed to an ASP page before writing to the output stream. Apply patches 1379 and 1381 through Expert Exchange.</p> <p>Affected Products Consona Live Assistance</p>

Consona Dynamic Agent
Consona Subscriber Assistance

3 Problem
Vulnerability to Remote (Client-Side) Arbitrary Code Execution

Description

Consona (*SupportSoft*) uses a proprietary site-locking mechanism through a plug-in license, which are embedded in all Web pages that use SupportSoft ActiveX controls. Consona generates this plug-in license and it is not possible to spoof it; however, by decoding the plug-in-license, a malicious user may obtain information regarding which URLs are allowed to host the ActiveX controls. The malicious user could then use this information, along with DNS hijacking, to host and use the ActiveX controls on a fake website that claims to be a legitimate one.

Impact Rating

Medium

Recommendation

- Host the website for ActiveX controls under HTTPS.
- For extra security, add allowed URL entries under registry on the user's machine:
 - HKLM\Software\SupportSoft\Security\Pluginlock

If this entry is present on the user's machine, other URLs (even those present in a valid plug-in license) would not be allowed to run ActiveX controls.

Affected Products

Consona Live Assistance
Consona Dynamic Agent
Consona Subscriber Assistance

4 Problem
Vulnerability to Local Privilege Escalation

Description

Consona (*SupportSoft*) Repair Service runs in System context to allow Support Actions, which are signed scripts released from the customer website, to perform actions that require higher access privileges. It is possible to create well-crafted packets, send them to Consona (*SupportSoft*) Repair Service, and execute code in a privileged mode.

Impact Rating

Medium

Recommendation

Communication between Consona (*SupportSoft*) controls and Repair Service would be encrypted with shared secret key generated on the user's machine. Install the fix when it becomes available.

Affected Products

- Consona Dynamic Agent
- Repair Manager
- Consona Subscriber Activation
- Subscriber Agent