

Ingres Security Alert

Communication Content

August 2011



August 30, 2011

Dear Valued Ingres Customer:

Information security is of utmost priority to Ingres. A new vulnerability has recently been identified in Ingres 10.0, 9.3, 9.2, 9.1, and 2.6. We have given this vulnerability a security threat level of 'Low' and recommend that the available security patches be applied as soon as possible, if applicable. This problem impacts only the Microsoft Windows platform.

Ingres event overflow using IIPROMPT* – bug 125598.

Description: An unauthenticated attacker can write to a shared memory segment and trigger an event to overflow data in the Ingres name server (iigcn).

Fixes are available for the current release of Ingres 10.0, 9.2, 9.1 and 2.6 versions on their respective platforms. The security fixes can be quickly applied with little to no anticipated impact to systems.

Ingres customers with a current support contract can review the following [knowledge base document](#) for information on downloading the available fixes.

We would like to additionally thank our community for bringing this vulnerability to our attention.

For more information about Ingres security alerts and to register to proactively receive these alerts via email please register at: <http://www.ingres.com/support/security-announcements.php>.

Regards,

Emma McGrattan
Senior Vice President, Engineering
Ingres Corporation
Emma.Mcgrattan@ingres.com

Pamela Fowler
VP of Worldwide Support/Security Vulnerabilities
Ingres Corporation
Pamela.Fowler@ingres.com