Ingres Security Alert

Communication Content

February 2010

February 26, 2010

Dear Valued Ingres Customer:

Information security is of utmost priority to Ingres. A new vulnerability has recently been identified in Ingres 9.1, Ingres 9.2, and Ingres 9.3. We have given this vulnerability a security threat level of 'Medium' and recommend that the available security patches be applied as soon as possible.

Fixes are available for the current release of Ingres 9.1, 9.2, and 9.3 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 subscription should contact Ingres Technical Support to obtain the latest patch.

We would like to additionally thank **Intevydis Blog** for bringing the following vulnerability to our attention.

Ingres remote user attack after SIGSEGV – bug 123208.

Description: A remote user can send specific data to the DBMS which triggers a SIGSEGV in memcpy() allowing a remote user to initiate a Denial of Service (DoS) attack.

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,

Bill Maimone
Senior Vice President, Engineering
Ingres Corporation

Pamela Fowler
VP of Worldwide Support/Security Vulnerabilities
Ingres Corporation