IOActive Security Advisory

Title	IBM Informix XML functions overflows
Severity	High
Discovered by	Ariel Matias Sanchez

Introduction

Informix is one of the world's most widely used database servers, with users ranging from the world's largest corporations to start-ups. Informix incorporates design concepts that are significantly different from traditional relational platforms, resulting in extremely high levels of performance and availability, distinctive capabilities in data replication and scalability, and minimal administrative overhead.

Informix contains two vulnerabilities affecting several versions. Exploitation of these vulnerabilities may allow execution of arbitrary code or cause denial of service (DoS).

Affected Products

All IBM Informix versions 11.50 prior to and including 11.50.xC9W2 – all platforms
All IBM Informix versions 11.70 prior to 11.70.xC7 – all platforms

This vulnerability affects only the following Informix products (informally known as "Informix Servers"):

- IBM Informix Choice Edition
- IBM Informix Developer Edition
- IBM Informix Express Edition
- IBM Informix Growth Edition
- IBM Informix Growth Warehouse Edition
- IBM Informix Innovator-C Edition
- IBM Informix Ultimate Edition
- IBM Informix Ultimate Warehouse Edition

Impact

Denial of Service / Remote Code Execution

Technical Details

IBM's Informix database server contains two XML functions “genxmlqueryhdr” and “genxmlquery” that suffer from buffer overflow vulnerabilities. These issues are due to insufficient bounds checking of arguments passed to the functions.

Successful exploitation may allow execution of arbitrary code or cause denial of service (DoS) against the instance.

To exploit the vulnerability the malicious user would need:

- Valid credential to connect to database

- CONNECT privilege on database

Solution

Upgrade to a version of Informix with the fix (later than 11.50.xC9W2; 11.70.xC7 or later).

CVE

More information can be found about this vulnerability at the following CVE location:

- http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-4857

Additional information

- http://www.ibm.com/support/docview.wss?rs=630&uid=swg21618994