

VulnWatch: [VulnWatch] IBM DB2 SATADMIN.SATENCRYPT buffer overflow (#NISR05012005E)

[VulnWatch] IBM DB2 SATADMIN.SATENCRYPT buffer overflow (#NISR05012005E)

Source: <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2005-01/0007.html>

From: NGSSoftware Insight Security Research (*nistr_at_nextgenss.com*)

Date: 01/05/05

To: <bugtraq@securityfocus.com>, <ntbugtraq@listserv.ntbugtraq.com>, <vulnwatch@vulnwatch.org>

Date: Wed, 5 Jan 2005 17:51:29 -0000

NGSSoftware Insight Security Research Advisory

Name: IBM DB2 SATADMIN.SATENCRYPT buffer overflow

Systems Affected: DB2 8.1

Severity: Medium risk from remote

Vendor URL: <http://www.ibm.com/>

Author: David Litchfield [david at ngssoftware.com]

Relates to: <http://www.nextgenss.com/advisories/db2-02.txt>

Date of Public Advisory: 5th January 2005

Advisory number: #NISR05012005E

Advisory URL: <http://www.ngssoftware.com/advisories/db205012005E.txt>

Description

IBM's DB2 database server, when configured for Satellite Administration includes a number of SQL functions. One of these, the SATENCRYPT function suffers from a stack based buffer overflow vulnerability.

Details

The SATENCRYPT function in the SATADMIN schema is vulnerable to a classic stack based overflow. The satencrypt function is exported by db2prom.dll and one of it's subfunctions creates a 40 byte buffer. User supplied data is copied to the buffer until a null terminator is reached in a while loop. By passing a parameter longer than 40 bytes allows the attacker to overflow the buffer and overwrite the saved return address. By exploiting this an attacker can gain elevated privileges.

Note – by default, public cannot execute this function.

Fix Information

IBM has written a patch and can be obtained with the latest fixpak.

<http://www-306.ibm.com/software/data/db2/udb/support/downloadv8.html> – DB2

VulnWatch: [VulnWatch] IBM DB2 SATADMIN.SATENCRYPT buffer overflow (#NISR05012005E)

v8.1

<http://www-306.ibm.com/software/data/db2/udb/support/downloadv7.html> – DB2

v7.x

NGSSQuirreL for DB2 (<http://www.nextgenss.com/db2.htm>) can be used to assess whether your DB2 server is vulnerable to this.

About NGSSoftware

NGSSoftware design, research and develop intelligent, advanced application security assessment scanners. Based in the United Kingdom, NGSSoftware have offices in the South of London and the East Coast of Scotland. NGSSoftware's sister company NGSConsulting, offers best of breed security consulting services, specialising in application, host and network security assessments.

<http://www.ngssoftware.com/>

Telephone +44 208 401 0070

Fax +44 208 401 0076

enquiries@ngssoftware.com