

MWR InfoSecurity Security
Advisory

IBM Informix Pre-
Authentication Stack
Overflow

14th April 2008



Contents

1	Detailed Vulnerability Description	5
1.1	Introduction	5
1.2	Technical Background.....	5
1.3	Vulnerability Details.....	6
1.4	Exploit Information	6
1.5	Dependencies	6
2	Recommendations.....	7

IBM Informix Pre-Authentication Stack Overflow

Package Name:	IBM Informix Dynamic Server
Date:	2008-04-14
Affected Versions:	Numerous versions of software are affected including: - IBM Informix IDS 7.x – 11.x Please refer to vendor links for exact version information of affected products.

CVE Reference	CVE-2008-0949
Date	14 th April 2008
Author	M. Ruks
Severity	High
Local/Remote	Remote
Vulnerability Class	Stack Based Overflow
Vendor URL	www.ibm.com
Version	A full list of affected versions can be obtained from the following location: - http://nvd.nist.gov/nvd.cfm?cvename=CVE-2008-0949
Vendor Response	The vendor has released updates to resolve this issue, please refer to the following links. http://www-1.ibm.com/support/search.wss?rs=0&q=IC55223&apar=only http://www-1.ibm.com/support/search.wss?rs=0&q=IC55224&apar=only http://www-1.ibm.com/support/search.wss?rs=0&q=IC55225&apar=only
Exploit Details Included	Yes
Affected OS	All supported Operating Systems are vulnerable.

Overview:

The IBM Informix Database service is vulnerable to a stack based buffer overflow which can be exploited remotely before the authentication has been completed.

Impact:

The vulnerability would enable an attacker to execute arbitrary code on the system with the privileges of the Informix user. By default, this account is a member of the administrators group on a Microsoft Windows system.

Cause:

The code responsible for parsing the parameters within the first packet of the protocol handshake does not validate the number of arguments it accepts. This results in the ability to overflow a stack buffer which in turn allows arbitrary code to be executed.

Interim Workaround:

Introduce host based or network filtering controls to restrict access to the affected service to authorised IP addresses only.

Solution:

The appropriate IBM fixes should be applied to affected systems, please refer to the links included above.

1 Detailed Vulnerability Description

1.1 Introduction

The Informix Dynamic Server database is developed by IBM and is described by the vendor as follows: -

“IBM Informix data servers are known worldwide for being exceptionally easy to manage while maintaining high availability and blazing online processing capabilities.”

Source: <http://www-306.ibm.com/software/data/informix/>

1.2 Technical Background

The product can be installed such that remote connections can be established to the database so that SQL queries can be executed and system administration can be performed. By default, a listener process runs on TCP port 1526 which is responsible for handling connections from clients. This service is primarily used to access the database to execute SQL queries.

The initial packet sent to the Informix listener by a client contains a series of parameters which will be passed to a server side process. These parameters are included within the packet and are separated by delimiter fields as can be observed in the following network traffic dump.

0030	44	e8	5d	6f	00	00	73	71	41	5a	34	42	50	51	41	41	D.]o..sq	AZ4BPQAA		
0040	73	71	6c	65	78	65	63	20	69	6e	66	6f	72	6d	69	78	sql	exec	informix	
0050	20	2d	70	70	61	73	73	77	6f	72	64	20	39	2e	33	30	-p	passwd	ord	9.30
0060	30	20	52	44	53	23	4e	30	30	30	30	30	30	20	2d	70	0	RDS#NO	00000	-p
0070	20	2d	66	49	45	45	45	49	20	44	42	50	41	54	48	3d	-F	EEEEI	DBPATH=	
0080	2f	2f	6f	6c	5f	76	6d	77	61	72	65	32	6b	20	44	42	///ot_vmw	are2k	DB	
0090	4d	4f	4e	45	59	3d	24	2e	20	43	4c	49	45	4e	54	5f	MONEY=\$.	CLIENT_		
00a0	4c	4f	43	41	4c	45	3d	65	6e	5f	55	53	2e	43	50	31	LOCALE=e	n_US.CP1		

The data highlighted in blue is a fixed string which must be sent at the start of the packet with the brown text indicating the string based arguments. The green highlighting is the delimiter field between each parameter (0x20 or space) and the separator between the variable name and its data (0x3d or equals sign).

When processing the packet the “oninit” process on the server is responsible for parsing the data and pushing pointers to each of the parameters to a data structure located on the stack.

The function which performs the parsing is responsible for performing a number of operations on the user supplied data. Within the parent parsing function a number of other specific parsing functions are called. The data supplied in the packet is stepped through character by character, if a 0x0a or 0x20 character is encountered it is replaced by the character 0x00 so that all strings are correctly null terminated. The function then checks the subsequent characters in the string to determine if they are either a 0x20 or 0x0a. If so the function steps over these characters one by one until another character is detected. A pointer to the next character in the string is then pushed to the stack which enables this parameter string to be referenced by another operation.



Once the pointer is pushed to the stack the function continues with the next character until the entire string has been processed. Once pointers to each parameter have been passed to the string a null word is pushed to the stack to terminate the data structure.

1.3 Vulnerability Details

A vulnerability was identified in this code when a large number of parameters, delimited by either a 0x20 or 0x0a, are sent in the initial packet. A stack based buffer overflow occurs in the outer parsing function as too many pointers are pushed to the stack and subsequently overwrite the function's return address.

When the function responsible for copying the pointers to the stack returns it continues through the parent parsing function. Control over execution is gained when the outer function returns. The execution conveniently continues at the location referenced by the pointer which was used to overwrite the return address.

This pointer references the start of the memory location where the parameter data sits and is written to the stack using the value in the ESI register. This means that it is not necessary to discover the location of the shellcode in memory as a pointer to its location is provided by the function itself. The shellcode can therefore be located in a parameter field of the initial data packet and will automatically be executed after the pointer has overwritten the return address.

1.4 Exploit Information

The vulnerability can be trivially exploited by a remote attacker if an initial packet containing an excessive number of parameters with the correct delimiter is supplied. The packet required to exploit the vulnerability requires a total of 83 delimiters to be sent. It would then be possible for an attacker to insert arbitrary shellcode

It is important to avoid the characters 0x20 and 0x0a in the shellcode as these will be converted to 0x00 by the parsing function. The entire packet must also be less than 230 bytes in length due to restrictions on the size of data which will be processed by the application.

The existence of this vulnerability has been confirmed by MWR InfoSecurity and working exploit code exists.

1.5 Dependencies

The impact of the vulnerability is dependent on the permissions of the Informix user under which the process is running. If this user has restricted permissions the impact of the issue is reduced; however, this is still a significant vulnerability.

2 Recommendations

It is recommended that the relevant fixes be applied to all affected systems in line with the information provided by the vendor. Information about fixes can be discovered at the following locations: -

<http://www-1.ibm.com/support/search.wss?rs=0&q=IC55223&apar=only>

<http://www-1.ibm.com/support/search.wss?rs=0&q=IC55224&apar=only>

<http://www-1.ibm.com/support/search.wss?rs=0&q=IC55225&apar=only>

To reduce the level of risk exposed to users of the software it is advised that the application be run under a user account with the lowest level of privileges. It is also recommended that Informix systems, especially those in production environments, be subject to network level filtering such that only trusted IP addresses can communicate with the service. It should be noted that this is a generic recommendation and is not specific to this technology.

MWR InfoSecurity
St. Clement House
1-3 Alencon Link
Basingstoke, RG21 7SB
Tel: +44 (0)1256 300920
Fax: +44 (0)1256 844083
mwrinfosecurity.com