

# [UNIX] IBM Informix Dynamic Server DBLANG Directory Traversal Vulnerability

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-11/msg00023.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxxx)>
  - *Date:* 12 Nov 2007 16:27:45 +0200
- 

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>  
-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.  
<http://www.securiteam.com/maillinglist.html>

-----

IBM Informix Dynamic Server DBLANG Directory Traversal Vulnerability

---

## SUMMARY

IBM Corp.'s <<http://www-306.ibm.com/software/data/informix/ids/>> Informix Dynamic Server is an online transaction processing data server. It contains several set-uid root binaries.

Local exploitation of a directory traversal vulnerability in IBM Corp.'s Informix Dynamic Server allows attackers to elevate privileges to root.

## DETAILS

Vulnerable Systems:

\* IBM Corp.'s Informix Dynamic Server version 10.00 UC6TL installed on a Linux system.

(Other versions are also suspected as vulnerable, versions for other supported Unix systems should also be considered vulnerable).

This vulnerability exists due to insufficient checking for directory traversal sequences when processing the DBLANG environment variable. By using values containing directory traversal specifiers, such as "../", an attacker can cause set-uid binaries to use Native Language Support (NLS)

## [UNIX] IBM Informix Dynamic Server DBLANG Directory Traversal Vulnerability

message files under their control.

Exploitation allows local attackers to gain root privileges. In order to exploit this vulnerability, an attacker would need access to execute one of the set-uid root binaries that utilizes the DBLANG environment variable.

Since an attacker can control NLS message file data, they are able to pass arbitrary format string arguments to the variable argument function printf(3). Consequently, this vulnerability can be exploited using publicly known format string exploitation techniques.

When attempting to exploit this vulnerability, it is likely that an attacker would try to execute code within area of memory that are considered data. As such, NX, XD, exec-shield, PAX and other data execution prevention technologies can decrease the likelihood of success.

### Workaround:

Removing the set-uid bit from all programs included with Informix will prevent exploitation. However, doing so may also disable functionality.

### Vendor Status:

IBM Corp. has addressed this vulnerability within version 10.00.xC7W1 of Informix Dynamic Server. For more information, visit the following URL.

<<http://www-1.ibm.com/support/docview.wss?uid=swg27011082>>  
<http://www-1.ibm.com/support/docview.wss?uid=swg27011082>

### CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5670>>  
CVE-2007-5670

### Disclosure Timeline:

- \* 09/01/2007 – Initial vendor notification
- \* 09/13/2007 – Initial vendor response
- \* 11/06/2007 – IBM Released 10.00.xC7W1
- \* 11/09/2007 – Public disclosure

## ADDITIONAL INFORMATION

The information has been provided by iDefense.

The original article can be found at:

<<http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=624>>  
<http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=624>

=====

[UNIX] IBM Informix Dynamic Server DBLANG Directory Traversal Vulnerability

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@xxxxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxxx

=====  
=====

**DISCLAIMER:**

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.