

The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:

5/01/2012

SUBJECT:

Vulnerability in Oracle Database Server 'TNS Listener' Could Allow Remote Code Execution

OVERVIEW:

A vulnerability has been discovered in the Oracle database server's 'TNS Listener' service, which could allow for multiple remote attacks against an Oracle database. This vulnerability may be remotely exploitable without authentication. Oracle database is an enterprise database server available for multiple operating systems. 'TNS Listener' is a component that routes connections from the client to the database server based on a naming convention (instance name).

Successful exploitation of this vulnerability could result in an attacker altering the naming convention and routing the database information to the attackers system.

SYSTEMS AFFECTED:

- Oracle Database 11g Release 2, versions 11.2.0.2, 11.2.0.3
- Oracle Database 11g Release 1, version 11.1.0.7
- Oracle Database 10g Release 2, versions 10.2.0.3, 10.2.0.4, 10.2.0.5

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: Low

DESCRIPTION:

A vulnerability has been discovered in the Oracle database server's 'TNS Listener' service. 'TNS Listener' is a component that routes connections from the client to the database server based on a naming convention (instance name). An attacker could exploit this vulnerability by sending a malicious request to the TNS Listener service and poisoning the data handled by 'TNS Listener'.

It should be noted that this vulnerability is remotely exploitable without authentication. A remote user can exploit this vulnerability to impact the confidentiality, integrity and availability of systems that do not have recommended solution applied.

Successful exploitation of this vulnerability could result in an attacker gaining the ability to reroute the TNS Listener' component of the vulnerable database server to the attackers system which may result in man-in-the-middle, session-hijacking, or denial-of-service attacks.

RECOMMENDATIONS:

The following actions should be taken:

- Patch vulnerable Oracle products immediately after appropriate testing.
- Block access to port 1521/TCP at the network perimeter, unless there is a valid business need to allow access.

REFERENCES:**Oracle:**

<http://www.oracle.com/technetwork/topics/security/alert-cve-2012-1675-1608180.html>

SecurityFocus:

<http://www.securityfocus.com/bid/53308>

CVE:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1675>