

Oracle Listener Control Format String Vulnerabilities (#NISR14082002)

Source: <http://www.derkeiler.com/Mailing-Lists/NT-Bugtraq/2002-08/0037.html>

From: NGSSoftware Insight Security Research (nisr@NEXTGENSS.COM)

Date: 08/14/02

Date: Wed, 14 Aug 2002 09:18:29 +0100
From: NGSSoftware Insight Security Research <nisr@NEXTGENSS.COM>
To: NTBUGTRAO@LISTSERV.NTBUGTRAO.COM

NGSSoftware Insight Security Research Advisory

Name: Oracle Listener Control Format Strings
Systems Affected: Oracle 9i, 8i on all platforms
Severity: Medium
Category: Format String Vulnerabilities
Vendor URL: <http://www.oracle.com/>
Authors: David Litchfield (david@ngssoftware.com)
Advisory URL: <http://www.ngssoftware.com/advisories/ora-lsnrfmtstr.txt>
Date: 14th August 2002
Advisory number: #NISR14082002
VNA Reference: <http://www.nextgenss.com/vna/ora-lsnrctl.txt>

Description

Oracle provide a tool called the Listener Control utility (lsnrctl) to allow an Oracle DBA to remotely control the Listener. The Listener is responsible for dealing with client requests for database services. This control utility contains an indirect remotely exploitable format string vulnerability.

Details

By default the Oracle Listener is not protected against unauthenticated access and control. The configuration files of Listeners in such a state can be modified without the user needing to supply a password. By modifying certain entries in the listener.ora file, by inserting a format string exploit, an attacker can gain control of a Listener control utility. Typically an attack would require the attacker to modify the file and wait for an Oracle DBA to use the Listener control utility to access the Listener at which point control over the utility's path of execution can be gained. This will give the attacker the ability only to gain control of the DBA's machine and not the database server. This is a complex attack and requires certain "events" to happen and as such the risk is quite low. That said, Oracle users are urged to apply the patch.

NT-Bugtraq: Oracle Listener Control Format String Vulnerabilities (#NISR14082002)

Fix Information

NGSSoftware alerted Oracle to this problem on the 13th May 2002. Oracle have produced a patch and issued an alert. Please see their bulletin for more details.

<http://otn.oracle.com/deploy/security/pdf/2002alert40rev1.pdf>

In the interim NGSSoftware advise that Oracle DBAs ensure that the Listener can not be controlled remotely and anonymously.

There are several steps one can take to secure the Listener and hence prevent exploitation of this format string vulnerability.

One can set in the listener.ora

ADMIN_RESTRICTIONS_Isnname=ON

This will prevent modifications to the Listener config files. Further a password should be set to limit actions a user can take.

-
- **Previous message:** <http-equiv@excite.com>: "[SAME LADY, DIFFERENT DRESS: Internet Explorer 6](#)"
 - **Next in thread:** [Aaron C. Newman: "Re: Oracle Listener Control Format String Vulnerabilities \(#NISR14082002\)"](#)
 - **Reply:** [Aaron C. Newman: "Re: Oracle Listener Control Format String Vulnerabilities \(#NISR14082002\)"](#)
 - **Messages sorted by:** [\[date \] \[thread \] \[subject \] \[author \] \[attachment \]](#)