

Re: Oracle Listener Control Format String Vulnerabilities (#NISR14082002)

Source: <http://www.derkeiler.com/Mailing-Lists/NT-Bugtraq/2002-08/0048.html>

From: David Litchfield (david@NGSSOFTWARE.COM)

Date: 08/16/02

Date: Fri, 16 Aug 2002 05:42:32 +0100
From: David Litchfield <david@NGSSOFTWARE.COM>
To: NTBUGTRAO@LISTSERV.NTBUGTRAO.COM

> >This is a complex attack and requires certain "events" to happen and as
> >such the risk is quite low."
>
> Actually, I think this attack is more serious than this. There is a
> RELOAD command that causes the listener to reread the listener.ora file,
> so an attacker would not need to wait for a DBA to restart the service
> and it would allow the attacker to gain full control of the database
> server.

The format string bug is in the listener control utility and not the actual listener so reloading the listener wont have any effect. That said, if an anonymous user can modify the listener.ora and other files through the listener then this can pose a problem where an attacker can run arbitrary commands. These were dicussed in Howard Smith's paper "Hack Proofing Oracle" <http://otn.oracle.com/deploy/security/pdf/oow00/orahack.pdf> .

Cheers,

David Litchfield

NGSSoftware Ltd

<http://www.ngssoftware.com/>

- **Previous message:** [David Litchfield: "Microsoft SQL Server Agent Jobs Vulnerabilities \(#NISR15002002B\)"](#)
- **In reply to:** [Aaron C. Newman: "Re: Oracle Listener Control Format String Vulnerabilities \(#NISR14082002\)"](#)
- **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)