

SECURITY ADVISORY 2006-10-01

Paros Proxy Default “sa” password Remote Command
Exec /Data Disclosure



Copyright and Disclaimer

The information in this advisory is Copyright 2006 FortConsult ApS. It is provided so that our customers and others understand the risk they may be facing by running affected software on their systems.

In case you wish to copy information from this advisory, you must either copy all of it or refer to this document.

No guarantee is provided for the accuracy of this information, or damage you may cause your systems in testing.

The Security Research Team

This advisory has been discovered by FortConsults Security Research Team/Andrew Christensen.

FortConsult is a specialist in technical services within the field of IT security. We are vulnerability experts that help business enterprises to protect themselves against the numerous security threats that exist today – both as impartial consultants and with responsibility for specific tasks. Our primary services are security tests and practically-oriented security consultancy.

For more information: www.fortconsult.net.

Issue Description

Paros is an intercepting HTTP/HTTPS proxy for use in security testing web applications.

Paros versions below 3.2.6 may contain a flaw where a remote attacker can connect to a database port opened on the machine running Paros.

The problem stems from use of a blank "sa" password on the open-source database ("HSQLDB") which is integrated with Paros.

The database server (which is also written in Java) contains functionality for executing arbitrary Java statements. This is how HSQLDB provides Stored Procedure functionality.

Impact of Successful Exploitation

The issue may result in disclosure of confidential data, and possible execution of commands on the victim machine.

A remote attacker may find credentials for web applications, valid session IDs, and confidential data downloaded from the website being tested with Paros. This information is present in the database.

Additionally, the possibility of executing Java statements on the database server may mean that an attacker can gain access to files or execute command at the OS level (by performing thenJava equivalent of a "system()" call).

History

October 3rd 2005: Problem discovered / reported

October 7th 2005: Issue re-reported via sourceforge, as mail appeared lost in transit

October 7th 2005: Paros developer releases corrected version

Countermeasures

Upgrade to version 3.2.6.

Firewall the host running Paros.

Demonstration

To demonstrate this, first start Paros on the victim host (here, 192.168.0.1).

Next, add the following lines to the file \$HOME/sqltool.rc on the attacking host (IP does not matter):

```
# connect to victimhost as sa, victimhost has IP 192.168.0.1
urlid victimhost-sa
url: jdbc:hsqldb:hsq://192.168.0.1
username sa
password
```

To connect using the "victimhost-sa" block above, ensure HSQLDB is installed, and run:

```
java -jar $HSQLDB_HOME/jsqldb.jar victimhost-sa
```

At this point, it is possible to pull data from the tables in the database (browsing state, history, credentials).

The page at <http://hsqldb.org/doc/guide/ch09.html#call-section> also states it is possible to execute Java statements by writing them in the format "java.lang.Math.sqrt"(2.0).

FORTCONSULT

Straight talk on IT security