

# [NEWS] DataRescue IDA Pro Remote Debugger Server Authentication Bypass Vulnerability

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-03/msg00050.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxx)>
  - *Date:* 26 Mar 2007 13:45:43 +0200
- 

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>  
-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.  
<http://www.securiteam.com/maillinglist.html>

-----

DataRescue IDA Pro Remote Debugger Server Authentication Bypass Vulnerability

---

## SUMMARY

DataRescue Inc.'s <<http://www.datarescue.com/idabase/index.htm>> IDA Pro is "a disassembler and debugger for Windows, Linux, or Macintosh. It supports multiple binary formats as well as many processor architectures".

Remote exploitation of a password bypass vulnerability in DataRescue Inc.'s IDA Pro Remote Debugger Server allows attackers to execute arbitrary code under the context of the user who is running the remote debugger server.

## DETAILS

Vulnerable Systems:

- \* Remote debugger server for Windows and Linux from IDA Pro versions 5.0 and 5.1.
- \* It is suspected that the MacOS X version and earlier versions are also affected.

Since version 4.8, IDA Pro supports remote debugging of x86/AMD64 Windows

## [NEWS] DataRescue IDA Pro Remote Debugger Server Authentication Bypass Vulnerability

PE applications and Linux ELF applications over TCP/IP networks. The IDA distribution ships with a debugger server for Windows, Linux, and (as of version 5.1) MacOS X.

The IDA Pro debugger server allows a user to specify a password for authentication by supplying the `-P` parameter. The vulnerability specifically exists in the `processor_request()` function. This function is used for the initial packet exchange as well as subsequent requests. This function did not ensure that the remote user has authenticated prior to calling the `perform_request()` function. As such, attacker requests sent prior to authenticating would be processed normally.

Exploitation of the described vulnerability allows attackers to execute arbitrary code under the context of the user who starts the remote debugger server.

It should be noted that the debugger server does not run as a service. It must be manually executed. Additionally, the remote debugger server can only handle one debugger session at a time. As such, this vulnerability can not be exploited while the debugger server is in use.

### Workarounds:

In order to reduce exposure to this vulnerability, the remote debugger server should not be left running when it is not in use.

Additionally, access to the port used by the remote debugger server could be blocked with the use of a firewall.

### Vendor Status:

"Since this vulnerability is in the open part of IDA, we provide the corrected source code for the modified files."

DataRescue Inc. has made the fix available at the following URL:  
<[http://www.datarescue.com/freefiles/ida\\_remdeb\\_fix\\_22032007.zip](http://www.datarescue.com/freefiles/ida_remdeb_fix_22032007.zip)>  
[http://www.datarescue.com/freefiles/ida\\_remdeb\\_fix\\_22032007.zip](http://www.datarescue.com/freefiles/ida_remdeb_fix_22032007.zip)

### Disclosure Timeline:

- \* 03/20/2007 – Initial vendor notification
- \* 03/20/2007 – Initial vendor response
- \* 03/23/2007 – Coordinated public disclosure

## ADDITIONAL INFORMATION

The information has been provided by iDefense.  
The original article can be found at:

<<http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=492>>  
<http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=492>

[NEWS] DataRescue IDA Pro Remote Debugger Server Authentication Bypass Vulnerability

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@xxxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxx

=====

=====

**DISCLAIMER:**

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.