

# [UNIX] Multiple SQL Injection Vulnerabilities in DeskPRO

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-10/0038.html>

---

**From:** SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

**Date:** 10/09/03

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: 9 Oct 2003 15:17:43 +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>

-----

Multiple SQL Injection Vulnerabilities in DeskPRO

---

## SUMMARY

<<http://www.deskpro.com/>> DeskPRO is "an integrated script to manage your customer sales and support". The DeskPRO product uses a SQL engine (MySQL) to store information.

The product contains multiple pages that do not adequately filter our user provided data, allowing a remote attacker to insert malicious SQL statements into existing ones.

## DETAILS

Vulnerable systems:

- \* DeskPRO version 1.1.0 and prior

Immune systems:

- \* DeskPRO version 1.1.2

Examples:

[http://vulsite.com/deskpro\\_v1/faq.php?cat=45'](http://vulsite.com/deskpro_v1/faq.php?cat=45)

[http://vulsite.com/deskpro\\_v1/faq.php?article=105'](http://vulsite.com/deskpro_v1/faq.php?article=105)

## Securiteam: [UNIX] Multiple SQL Injection Vulnerabilities in DeskPRO

[http://vulsite.com/deskpro\\_v1/view.php?ticketid=1'&ticket\\_pass=](http://vulsite.com/deskpro_v1/view.php?ticketid=1'&ticket_pass=)

The vulnerability is better emphasized by the fact that a remote attacker can logon into the system with the administrator username without knowing the password by entering the following information in the logon screen:

Email: admin  
Password: 'or"='

Vendor response:

On the 21st of Sep 2003 this issue was reported to DeskPRO, the following reply was received on the same day:

Thank you for the notification, we will have a fix within 24 hours. We appreciate keeping the information out of the public domain until we have had time to fix and release a patch."

On the 2nd of Oct 2003 after the majority of their customers patched the issue, we have decided to release this advisory.

### ADDITIONAL INFORMATION

The information has been provided by <mailto:expert@securiteam.com>  
SecurITeam Experts.

=====

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@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

### 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.