

# [NEWS] eyeOS Remote Code Execution

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-02/msg00031.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxx)>
  - *Date:* 8 Feb 2006 18:52:28 +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>

-----

eyeOS Remote Code Execution

---

## SUMMARY

" <<http://www.eyeos.org/>> eyeOS is a web based operating system."

Remote Code Execution in eyeOS allows unauthenticated attackers to execute arbitrary PHP commands.

## DETAILS

Vulnerable Systems:

- \* eyeOS version 0.8.9 and prior

Immune Systems:

- \* eyeOS version 0.8.10

There is a Remote Code Execution vulnerability in eyeOS that is the result of improperly initializing users sessions.

```
if (!isset($_SESSION))  
session_start ();
```

The above code is taken from desktop.php @ lines 20–21 and is the reason

[NEWS] eyeOS Remote Code Execution

code execution is possible. The \$\_SESSION array is like any other variable until initialized with session\_start() unless session.auto\_start is set to 1. What's even worse is that obviously an attacker does not have to authenticate in order to exploit this issue, which makes it much more dangerous.

[http://eyeOS/desktop.php?baccio=eyeOptions.eyeapp&a=eyeOptions.eyeapp& SESSION\[usr\]=root& SESSION\[app](http://eyeOS/desktop.php?baccio=eyeOptions.eyeapp&a=eyeOptions.eyeapp& SESSION[usr]=root& SESSION[app)

The above URL will successfully execute the phpinfo() command on the target web-server with privileges of the web-server.

ADDITIONAL INFORMATION

The information has been provided by <<mailto:security@xxxxxxxxxxxxx>> GulfTech Security.

The original article can be found at:

<[http://www.gulftech.org/?node=research&article\\_id=00096-02072006](http://www.gulftech.org/?node=research&article_id=00096-02072006)>  
[http://www.gulftech.org/?node=research&article\\_id=00096-02072006](http://www.gulftech.org/?node=research&article_id=00096-02072006)

=====

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

=====  
=====

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.