

# [UNIX] SquirrelMail S/MIME Plugin Command Injection

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-02/0075.html>

---

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

**Date:** 02/17/05

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

Date: 17 Feb 2005 19:36:01 +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>

-----

SquirrelMail S/MIME Plugin Command Injection

---

## SUMMARY

Squirrelmail S/MIME plugin 'enables the viewing of S/MIME-signed messages of the MIME "multipart/signed" format'. Remote exploitation of a command injection vulnerability in the Squirrelmail S/MIME plugin allows web mail users to execute arbitrary commands with the privileges of the web server.

## DETAILS

Vulnerable Systems:

- \* SquirrelMail S/MIME plugin version 0.5 and prior

Immune Systems:

\*

The problem specifically exists due to insufficient filtering of user-provided data in a call to `exec()`. The following snippet exposes the offending area of code from `viewcert.php`:

```
if(!isset($cert)) $cert=$_GET['cert'];
```

```
...
```

## Securiteam: [UNIX] SquirrelMail S/MIME Plugin Command Injection

```
function x509_open($cert) {
    global $cert_in_dir, $openssl;
    $lines = array();
    exec("$openssl x509 -in $cert_in_dir$cert -subject -issuer \
        -dates -serial -fingerprint -noout 2>/tmp/err", $lines);
    ...
    list ($ow, $is, $nb, $na, $sn, $fp) = x509_open($cert);
}
```

The variable '\$cert' from the above snippet contains unfiltered user supplied data and can be exploited.

### Analysis:

Successful exploitation allows authenticated web mail users to execute arbitrary commands on the underlying system with the privileges of the web server. This can lead to further compromise and exposure of other users' mail to the attacker.

### Workaround:

PHP provides the `escapeshellarg()` routine to filter data to be used as an argument to calls such as `exec()` and `system()`. Modify the call to `exec()` from:

```
exec("$openssl x509 -in $cert_in_dir$cert -subject -issuer -dates \
    -serial -fingerprint -noout 2>/tmp/err", $lines);
```

### To:

```
$filtered = escapeshellarg("$cert_in_dir$cert");
exec("$openssl x509 -in $filtered -subject -issuer -dates -serial \
    -fingerprint -noout 2>/tmp/err", $lines);
```

### Vendor response:

The vendor has released S/MIME plugin 0.6 to address this vulnerability.

The plugin is available for download at:

[http://www.squirrelmail.org/plugin\\_view.php?id=54](http://www.squirrelmail.org/plugin_view.php?id=54)

[http://www.squirrelmail.org/plugin\\_view.php?id=54](http://www.squirrelmail.org/plugin_view.php?id=54)

### Disclosure Timeline:

09/22/2004 – Initial vendor notification

09/22/2004 – Initial vendor response

02/07/2005 – Coordinated public disclosure

### ADDITIONAL INFORMATION

The information has been provided by

<mailto:customerservice@idefense.com> iDEFENSE.

The original article can be found at:

<http://www.idefense.com/application/poi/display?id=191&type=vulnerabilities>

<http://www.idefense.com/application/poi/display?id=191&type=vulnerabilities>

=====

Securiteam: [UNIX] SquirrelMail S/MIME Plugin Command Injection

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.