

# SquirrelMail S/MIME Plugin Command Injection Vulnerability

iDEFENSE Security Advisory 02.07.05:

## I. BACKGROUND

Squirrelmail S/MIME plugin enables the viewing of S/MIME-signed messages of the MIME "multipart/signed" format. More information about the plugin is available at:

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

## II. DESCRIPTION

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.

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'];
...
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.

## III. 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.

## IV. DETECTION

iDEFENSE has confirmed the existence of this vulnerability in S/MIME plugin 0.5 and 0.4. Earlier versions are also suspected to be vulnerable.

## V. 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);
```

## **VI. 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)

## **VII. CVE INFORMATION**

The Common Vulnerabilities and Exposures (CVE) project has assigned the names CAN-2005-0239 to these issues. This is a candidate for inclusion in the CVE list (<http://cve.mitre.org>), which standardizes names for security problems.