Security Advisory SWRX-2015-003

Lastline Portal Session Fixation

Dell SecureWorks Counter Threat Unit™ Threat Intelligence

Advisory Information

Title: Lastline Portal Session Fixation
Advisory ID: SWRX-2015-003
Advisory URL: http://www.secureworks.com/cyber-threat-intelligence/advisories/SWRX-2015-003
Date published: Monday, June 8, 2015
CVE: CVE-2015-4126
CVSS v2 base score: 5.1
Date of last update: Monday, June 8, 2015
Vendors contacted: Lastline
Release mode: Coordinated
Discovered by: Dana James Traversie and Sean Wright, Dell SecureWorks

Summary

Lastline is a breach detection platform that provides administrative functionality and other features via a dedicated web application. A vulnerability in the Lastline Portal web application results from insufficient or improper session management in the web application or container. An unauthenticated, remote attacker could conduct session fixation attacks by persuading a user to follow a malicious link or visit an attacker-controlled website.

Affected products

This vulnerability has been confirmed in version 6.0.1 of the Lastline Portal web application.

Note: The Lastline infrastructure hosted by Dell SecureWorks is not vulnerable to this issue.

Vendor information, solutions, and workarounds

The vendor released an updated version of the Lastline Portal web application to address this vulnerability. Users should upgrade to version 6.3 or later.

Details

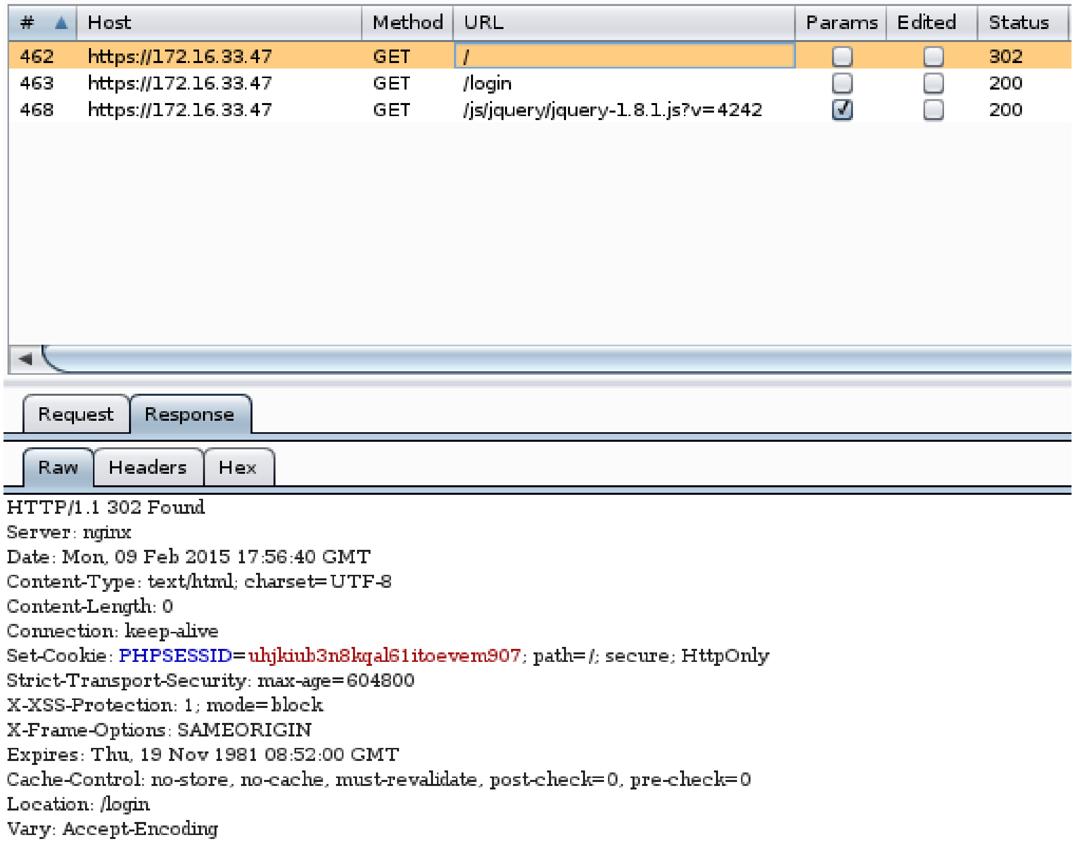
In version 6.0.1 of the Lastline Portal web application, session identifiers are not regenerated after a user successfully authenticates. An attacker could leverage this vulnerability to conduct session fixation attacks against users. Successful exploitation may allow an attacker to obtain complete control over the web application, modify or steal data, or launch additional attacks.

CVSS severity (version 2.0)

Access vector: Network
Access complexity: High
Authentication: None
Impact type: Gain privileges/assume identity, bypass protection mechanisms, read application data, modify application data, cause a denial of service
Confidentiality impact: Partial
Integrity impact: Partial
Availability impact: Partial
CVSS v2 base score: 5.1
CVSS v2 impact subscore: 6.4
CVSS v2 exploitability subscore: 4.9
CVSS v2 vector: (AV:N/AC:H/Au:N/C:P/I:P/A:P)

Proof of concept

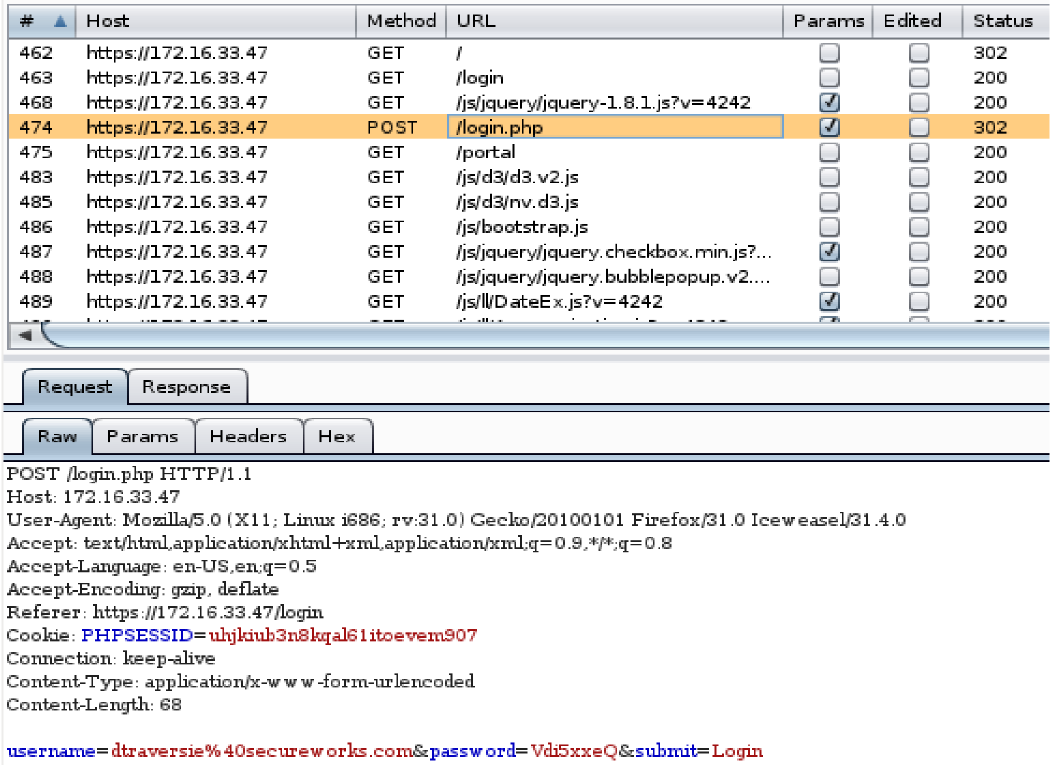
Figures 1 through 4 show the session identifier failing to regenerate after a user successfully authenticates. Dell SecureWorks researchers created a proof-of-concept video that illustrates the vulnerability, a working exploit, and its outcome.



# ▲	Host	Method	URL	Params	Edited	Status
462	https://172.16.33.47	GET	/	☐	☐	302
463	https://172.16.33.47	GET	/login	☐	☐	200
468	https://172.16.33.47	GET	/js/jquery/jquery-1.8.1.js?v=4242	☑	☐	200

```
HTTP/1.1 302 Found
Server: nginx
Date: Mon, 09 Feb 2015 17:56:40 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 0
Connection: keep-alive
Set-Cookie: PHPSESSID=uhjkiub3n8kqal61itoevem907; path=/; secure; HttpOnly
Strict-Transport-Security: max-age=604800
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Location: /login
Vary: Accept-Encoding
```

Figure 1. User browses to the Lastline Portal and is issued a session identifier associated with a new, unauthenticated session. (Source: Dell SecureWorks)

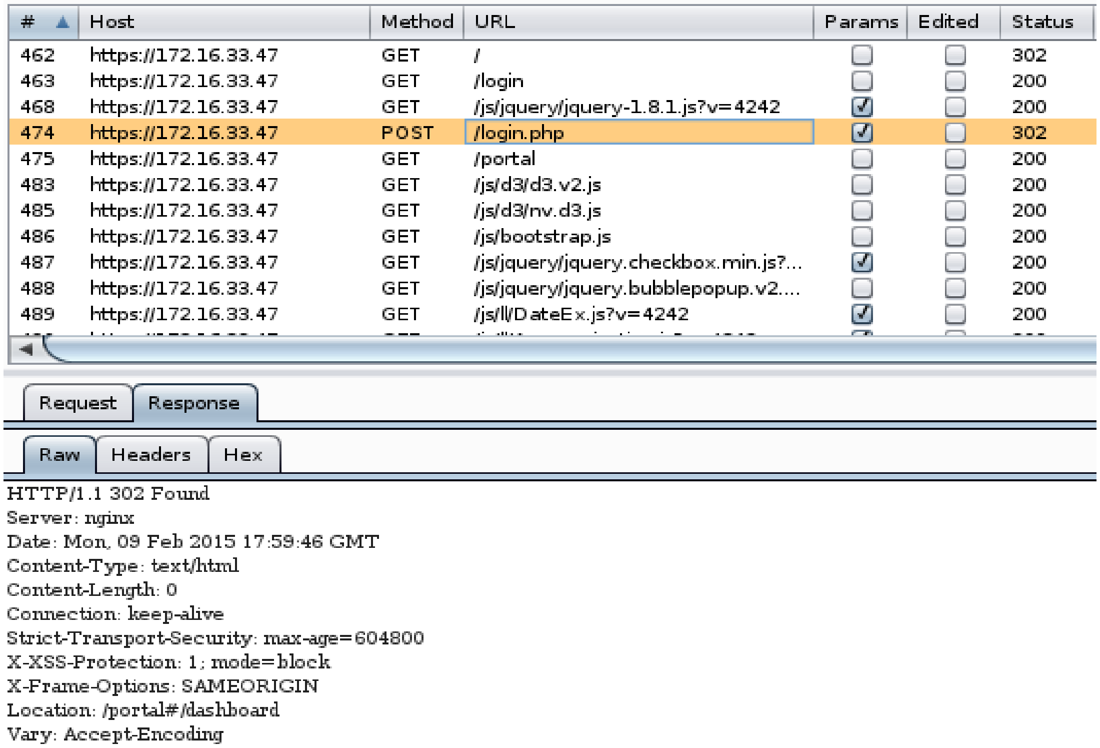


# ▲	Host	Method	URL	Params	Edited	Status
462	https://172.16.33.47	GET	/	☐	☐	302
463	https://172.16.33.47	GET	/login	☐	☐	200
468	https://172.16.33.47	GET	/js/jquery/jquery-1.8.1.js?v=4242	☑	☐	200
474	https://172.16.33.47	POST	/login.php	☑	☐	302
475	https://172.16.33.47	GET	/portal	☐	☐	200
483	https://172.16.33.47	GET	/js/d3/d3.v2.js	☐	☐	200
485	https://172.16.33.47	GET	/js/d3/nv.d3.js	☐	☐	200
486	https://172.16.33.47	GET	/js/bootstrap.js	☐	☐	200
487	https://172.16.33.47	GET	/js/jquery/jquery.checkbox.min.js?...	☑	☐	200
488	https://172.16.33.47	GET	/js/jquery/jquery.bubblepopup.v2....	☐	☐	200
489	https://172.16.33.47	GET	/js/ll/DateEx.js?v=4242	☑	☐	200

```
POST /login.php HTTP/1.1
Host: 172.16.33.47
User-Agent: Mozilla/5.0 (X11; Linux i686; rv:31.0) Gecko/20100101 Firefox/31.0 Iceweasel/31.4.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://172.16.33.47/login
Cookie: PHPSESSID=uhjkiub3n8kqal61itoevem907
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 68

username=dtraversie%40secureworks.com&password=Vdi5xxeQ&submit=Login
```

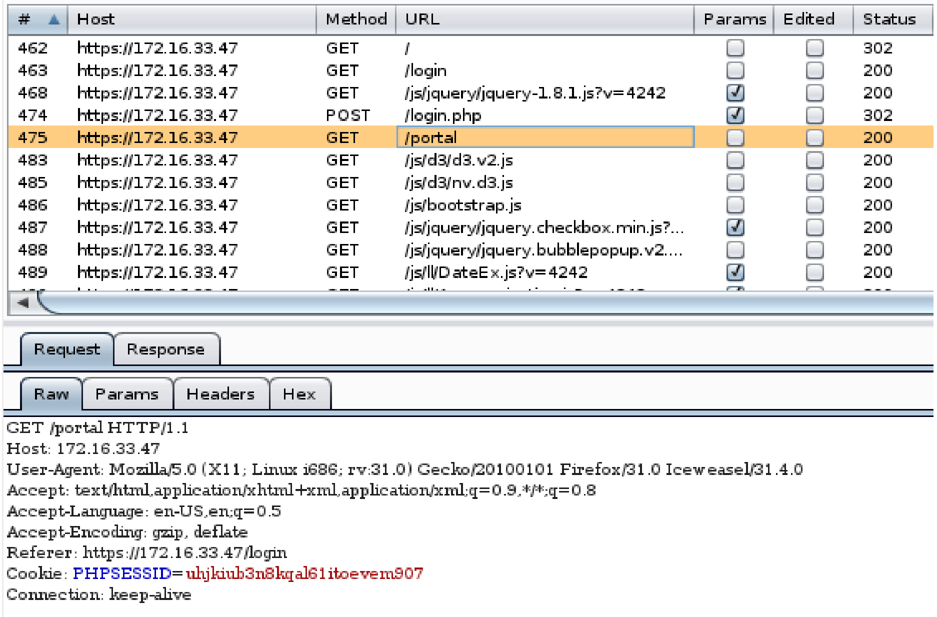
Figure 2. User submits credentials to the Lastline Portal. (Source: Dell SecureWorks)



# ▲	Host	Method	URL	Params	Edited	Status
462	https://172.16.33.47	GET	/	☐	☐	302
463	https://172.16.33.47	GET	/login	☐	☐	200
468	https://172.16.33.47	GET	/js/jquery/jquery-1.8.1.js?v=4242	☑	☐	200
474	https://172.16.33.47	POST	/login.php	☑	☐	302
475	https://172.16.33.47	GET	/portal	☐	☐	200
483	https://172.16.33.47	GET	/js/d3/d3.v2.js	☐	☐	200
485	https://172.16.33.47	GET	/js/d3/nv.d3.js	☐	☐	200
486	https://172.16.33.47	GET	/js/bootstrap.js	☐	☐	200
487	https://172.16.33.47	GET	/js/jquery/jquery.checkbox.min.js?...	☑	☐	200
488	https://172.16.33.47	GET	/js/jquery/jquery.bubblepopup.v2....	☐	☐	200
489	https://172.16.33.47	GET	/js/ll/DateEx.js?v=4242	☑	☐	200

```
HTTP/1.1 302 Found
Server: nginx
Date: Mon, 09 Feb 2015 17:59:46 GMT
Content-Type: text/html
Content-Length: 0
Connection: keep-alive
Strict-Transport-Security: max-age=604800
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
Location: /portal#/dashboard
Vary: Accept-Encoding
```

Figure 3. User authenticates successfully and is redirected to the dashboard landing page. (Source: Dell SecureWorks)



# ▲	Host	Method	URL	Params	Edited	Status
462	https://172.16.33.47	GET	/	□	□	302
463	https://172.16.33.47	GET	/login	□	□	200
468	https://172.16.33.47	GET	/js/jquery/jquery-1.8.1.js?v=4242	☑	□	200
474	https://172.16.33.47	POST	/login.php	☑	□	302
475	https://172.16.33.47	GET	/portal	□	□	200
483	https://172.16.33.47	GET	/js/d3/d3.v2.js	□	□	200
485	https://172.16.33.47	GET	/js/d3/nv.d3.js	□	□	200
486	https://172.16.33.47	GET	/js/bootstrap.js	□	□	200
487	https://172.16.33.47	GET	/js/jquery/jquery.checkbox.min.js?...	☑	□	200
488	https://172.16.33.47	GET	/js/jquery/jquery.bubblepopup.v2....	□	□	200
489	https://172.16.33.47	GET	/js/ll/DateEx.js?v=4242	☑	□	200

```
GET /portal HTTP/1.1
Host: 172.16.33.47
User-Agent: Mozilla/5.0 (X11; Linux i686; rv:31.0) Gecko/20100101 Firefox/31.0 Iceweasel/31.4.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://172.16.33.47/login
Cookie: PHPSESSID=uhjkiub3n8kqal61itoevem907
Connection: keep-alive
```

Figure 4. User browses to the dashboard landing page using the authenticated session. Note that the session identifier value did not change. (Source: Dell SecureWorks)

Revision history

1.0 2015-06-08: Initial advisory release

PGP keys

This advisory has been signed with the Dell SecureWorks Counter Threat Unit™ PGP key, which is available for download at http://www.secureworks.com/SecureWorksCTU.asc.

About Dell SecureWorks

Dell Inc. listens to clients and delivers worldwide innovative technology and business solutions they trust and value. Recognized as an industry leader by top analysts, Dell SecureWorks provides world-class information and IT security services to help organizations of all sizes protect their IT assets, comply with regulations and reduce security costs.

Disclaimer

This advisory may not be edited or modified in any way without the express written consent of Dell SecureWorks. Permission is hereby granted to link to this advisory via the Dell SecureWorks website or use in accordance with the fair use doctrine of U.S. copyright laws. See the Dell SecureWorks terms of use at http://www.secureworks.com/contact/terms_of_use/ for additional information.

The most recent version of this advisory may be found on the Dell SecureWorks website at http://www.secureworks.com. The contents of this advisory may change or be removed from the website without notice. Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. ANY USE OF THIS INFORMATION IS AT THE USER'S RISK. In no event shall Dell SecureWorks be liable for any damages whatsoever arising out of or in connection with the use or further publication or disclosure of this information.