



Logged in as: *jan.s.lewis* (Jan Lewis - administrator) 07-05-2012 14:01 UTC Project: AWS



[All Projects](#) | [Archive](#) | [Archive NTOP '11](#): [1\) Customer and Partners](#), [2\) Products and Services](#), [3\) Information Systems](#), [4\) Science and Technology](#), [5\) People and Organizational Culture](#), [6\) Business Processes](#) | [AWS](#) | [CM Request for Change - AWS](#) | [Requests: CM Request for Change](#), [Document Request for Change](#), [Equipment Retirement](#), [New Ideas](#), [Procurement Request](#), [Schedule Request](#) | [RFC's Completed](#) | [Trouble Ticket](#)

[Main](#) | [My View](#) | [View Issues](#) | [Report Issue](#) | [Change Log](#) | [Roadmap](#) | [Summary](#) | [Docs](#) | [Manage](#) | [Edit News](#) | [My Account](#) | [Plugins](#) | [Search](#) | [Bugtracker Hierarchy](#) | [Logout](#)

Recently Visited: [0011641](#)

Viewing Issue Advanced Details [ [Jump to Notes](#) ] [ [Send a reminder](#) ] [ [Export](#) ] [ [View Simple](#) ] [ [Issue History](#) ] [ [Print](#) ]

| ID                 | Category                                                     | Severity           | Reproducibility | Date Submitted       | Last Update       |
|--------------------|--------------------------------------------------------------|--------------------|-----------------|----------------------|-------------------|
| 0011641            | [CM Request for Change - AWS] 22.1.2)<br>AviationWeather.gov | major              | always          | 06-27-12<br>17:24    | 07-05-12<br>13:57 |
| <b>Reporter</b>    | Adrian Noland                                                | <b>View Status</b> | public          |                      |                   |
| <b>Assigned To</b> | Adrian Noland                                                |                    |                 |                      |                   |
| <b>Priority</b>    | immediate                                                    | <b>Resolution</b>  | open            | <b>Platform</b>      |                   |
| <b>Status</b>      | assigned                                                     |                    |                 | <b>OS</b>            |                   |
| <b>Projection</b>  | none                                                         |                    |                 | <b>OS Version</b>    |                   |
| <b>ETA</b>         | none                                                         |                    |                 | <b>Product Build</b> |                   |

**Summary** 0011641: Cross Site Scripting Vulnerabilities

#### Description

----- Forwarded message -----  
 From: \*Chris Hornbrook\* <[chris.f.hornbrook@noaa.gov](mailto:chris.f.hornbrook@noaa.gov)>  
 <<mailto:chris.f.hornbrook@noaa.gov>>>  
 Date: Tue, Jun 26, 2012 at 5:36 PM  
 Subject: NOAA Aviation Weather XSS  
 To: Sean Wink <[sean.wink@noaa.gov](mailto:sean.wink@noaa.gov)> <<mailto:sean.wink@noaa.gov>>>, Graham Stork <[graham.stork@noaa.gov](mailto:graham.stork@noaa.gov)> <<mailto:graham.stork@noaa.gov>>>

Saw this article that mentions that the NOAA Aviation Weather site has XSS vulnerabilities:

<http://news.softpedia.com/news/Team-Digi7al-Leaks-Data-from-San-Jose-State-University-Stanford-Others-277614.shtml> [^]

#### Steps To Reproduce

#### Additional Information

Contact Form Submission

You received a new contact form submission from:

- Name: Benjamin Hendel
- Email Address: [bthendel@mchsi.com](mailto:bthendel@mchsi.com)
- Subject: XSS Vulnerability

Message

It has come to my attention that your site is vulnerable to an XSS attack. Here's all the proof you need: <http://www.freeimagehosting.net/zpe7v> [^] And here's where I got this picture from: <http://www.hackforums.net/showthread.php?tid=2620977&pid=23883164#pid23883164>And [^] here is the person who posted it: <http://www.hackforums.net/member.php?action=profile&uid=760598> [^] If you still don't believe me, their is a very long list of pages vulnerable to XSS below. Good luck. image: url(javascript:alert('XSS'))">&loc=<http://www.facebook.com/US.NOAA.AviationWeatherCenter> [^]  
<http://aviationweather.gov/jump/?dl=4&site=Aviation%20Weather%20on%20Facebook&loc=> [^]  
">  
[http://aviationweather.gov/jump/?dl=4&site=Aviation%20Weather%20on%20Facebook&loc=">](http://aviationweather.gov/jump/?dl=4&site=Aviation%20Weather%20on%20Facebook&loc=) [^]  
[http://aviationweather.gov/jump/?dl=4&site=Aviation%20Weather%20on%20Facebook&loc=">](http://aviationweather.gov/jump/?dl=4&site=Aviation%20Weather%20on%20Facebook&loc=) [^]  
[http://aviationweather.gov/jump/?dl=4&site=Aviation%20Weather%20on%20Facebook&loc=">](http://aviationweather.gov/jump/?dl=4&site=Aviation%20Weather%20on%20Facebook&loc=) [^]  
">";!--"\* \* =&{()}  
[http://aviationweather.gov/jump/?dl=4&site=Aviation%20Weather%20on%20Facebook&loc=">](http://aviationweather.gov/jump/?dl=4&site=Aviation%20Weather%20on%20Facebook&loc=) [^]  
">  
[http://aviationweather.gov/jump/?dl=4&site=Aviation%20Weather%20on%20Facebook&loc=">](http://aviationweather.gov/jump/?dl=4&site=Aviation%20Weather%20on%20Facebook&loc=) [^]  
">

**Tags** No tags attached.

**Attach Tags** (Separate by ',') Existing tags

**TIN Required? (If "YES" please upload)**

**Deadline** 07-05-12

**Disposition**

**Configuration Change Authority** ASB Chief

**Disposition Date** 07-05-12

**Level of Change** Level 2 (Moderate)

**Change Notification**

**Attached Files**



Users sponsoring this issue

Sponsor issue

Hours

Relationships

New relationship

Current issue

parent of

Upload File

Select File

(Max size: 5,000k)

no file selected

Users monitoring this issue

User List

Adrian Noland, Bob Maxson, Clinton Wallace, Dan Vietor, David Bright, Jan Lewis, John Sereno, Larry Greenwood, Steve Chance

Add Note

Note

View Status

private

Notes

(0030355)

David Bright (manager)

07-05-12 13:19

Approved for release 7/5/2012.

(0030346)

Adrian Noland (developer)

07-02-12 18:04

edited on: 07-03-12 19:01

Summary:

It was reported that the CAWS site was vulnerable to XSS attacks. This could allow a malicious user to use [www.aviationweather.gov](http://www.aviationweather.gov) as a vector in attacks on end users.

An initial report was made on Dec11 at <http://www.xssed.com/mirror/74530/> [^] that we found after we began researching the problem. We found further evidence in the resources sent from the user contact form. An audit found more vulnerable pages.

|                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                          | <p>Files changed:</p> <p>library/AWC/Application/Controller/Plugin/XssFilter.php<br/>application/configs/application.ini<br/>application/modules/default/controllers/ErrorController.php<br/>application/modules/default/views/scripts/error/illegalparam.phtml<br/>application/modules/popups/controllers/TafsmetarsController.php<br/>application/modules/adds/controllers/IcingController.php<br/>application/modules/adds/controllers/PhputilsController.php<br/>application/modules/adds/views/scripts/phputils/airportweather.phtml<br/>application/modules/adds/controllers/DataController.php<br/>doc-root/exp/pirep_submit/select.php<br/>doc-root/exp/pirep_submit/accesslist.php<br/>doc-root/exp/ellrod/info.php<br/>doc-root/exp/ellrod/rap/index.php<br/>doc-root/exp/ellrod/ruc/index.php<br/>doc-root/exp/ellrod/nam/index.php<br/>doc-root/gis/makepirepkml.php<br/>doc-root/jump/index.php<br/>doc-root/testbed/afd/index.php<br/>doc-root/testbed/cwsu/tafboard/additional.php<br/>doc-root/testbed/cwsu/tafboard/index.php<br/>doc-root/testbed/cwsu/tafboard/tafboard_nomenu.php<br/>doc-root/testbed/cwsu/tafboard/tstation.php<br/>doc-root/testbed/cwsu/tafboard/tstation_nomenu.php<br/>doc-root/testbed/cwsu/tstatus/index.php<br/>doc-root/testbed/avwx/index.php<br/>doc-root/testbed/cwsu/tstatus/tstatus_nomenu.php<br/>doc-root/testbed/globalgrids/displaygrid.php<br/>doc-root/testbed/wxoutlook/index.php</p> <p>Technical Impact:<br/>High: Many pages were modified as a result of the audit as well as a front<br/>crontroller plugin (XssFilter.php) to make sure all areas of user input are clean.</p> <p>User Impact:<br/>High: The changes will prevent www.aviationweather.gov from being used as an<br/>attack vector.</p> <p>Testing:<br/>The reported page was /products/tafs and /products/metars. Further analysis found<br/>the airport weather lookup on front page as well as some other pages that were<br/>vulnerable. Using the string '/'&gt;&lt;script&gt;alert('Xss ByAtm0n3r')&lt;/script&gt;' in any of<br/>the page queries should, at a minimum, not execute the javascript alert, and in<br/>most cases show an error page.</p> |
| <p>(0030345)<br/><b>Adrian Noland</b> (developer) [<br/>private ]<br/>07-02-12 17:49</p> | <p>[anoland@nolandlx awc]\$ svn up<br/>U doc-root/exp/ellrod/rap/index.php<br/>U doc-root/exp/ellrod/ruc/index.php<br/>U doc-root/exp/ellrod/nam/index.php</p> <p>Fetching external item into 'library/AWC'<br/>Updated external to revision 1499.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <p>(0030336)<br/><b>Adrian Noland</b> (developer) [<br/>private ]<br/>06-29-12 21:12</p> | <p>[anoland@nolandlx AWC]\$ svn ci -m 'using different redirect'<br/>Sending Application/Controller/Plugin/XssFilter.php<br/>Transmitting file data .<br/>Committed revision 1496.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

|                                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|----------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                            | [anoland@nolandlx awc]\$ svn ci -m 'dont need as much for this error'<br>Sending application/modules/default/controllers/ErrorController.php<br>Transmitting file data .<br>Committed revision 1497.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| (0030333)<br><b>Adrian Noland</b> (developer) [private ]<br>06-29-12 15:57 | [anoland@nolandlx awc]\$ svn ci -m 'only params on icing page'<br>application/modules/adds/controllers/IcingController.php<br>Sending application/modules/adds/controllers/IcingController.php<br>Transmitting file data .<br>Committed revision 1494.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| (0030328)<br><b>Adrian Noland</b> (developer) [private ]<br>06-28-12 20:35 | [anoland@nolandlx awc]\$ svn ci -m 'filtering input on tafs/metars';<br>Sending application/modules/popups/controllers/TafsmetarsController.php<br>Transmitting file data .<br>Committed revision 1493.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| (0030321)<br><b>Adrian Noland</b> (developer) [private ]<br>06-28-12 18:52 | svn ci -m 'filtering POST vars';<br>Sending application/modules/adds/controllers/PhputilsController.php<br>Sending application/modules/adds/views/scripts/phputils/airportweather.phtml<br>Sending doc-root/exp/pirep_submit/accesslist.php<br>Sending doc-root/exp/pirep_submit/select.php<br>Sending doc-root/testbed/avwx/index.php<br>Sending doc-root/testbed/cwsu/tstatus/tstatus_nomenu.php<br>Sending doc-root/testbed/globalgrids/displaygrid.php<br>Sending doc-root/testbed/wxoutlook/index.php<br>Transmitting file data .....<br>Committed revision 1492.                                                                                                                                                                                                                                           |
| (0030320)<br><b>Adrian Noland</b> (developer) [private ]<br>06-28-12 18:31 | Performing status on external item at 'library/AWC'<br>[anoland@nolandlx awc]\$ svn ci -m 'XSS fixes'<br>Sending application/configs/application.ini<br>Sending application/modules/default/controllers/ErrorController.php<br>Sending doc-root/exp/pirep_submit/select.php<br>Sending doc-root/gis/makepirepkml.php<br>Sending doc-root/jump/index.php<br>Sending doc-root/testbed/afd/index.php<br>Sending doc-root/testbed/cwsu/tafboard/additional.php<br>Sending doc-root/testbed/cwsu/tafboard/index.php<br>Sending doc-root/testbed/cwsu/tafboard/tafboard_nomenu.php<br>Sending doc-root/testbed/cwsu/tafboard/tstation.php<br>Sending doc-root/testbed/cwsu/tafboard/tstation_nomenu.php<br>Sending doc-root/testbed/cwsu/tstatus/index.php<br>Transmitting file data .....<br>Committed revision 1491. |
| (0030319)<br><b>Adrian Noland</b> (developer) [private ]<br>06-28-12 18:31 | [anoland@nolandlx AWC]\$ svn ci -m 'adding new plugin controller; side menu change'<br>Adding Application/Controller/Plugin/XssFilter.php<br>Sending Application/View/scripts/Sidebar.phtml<br>Transmitting file data ..<br>Committed revision 1490.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| (0030296)<br><b>Adrian Noland</b> (developer)                              | <i>Reminder sent to: Bob Maxson, Clinton Wallace, Dan Vietor, David Bright, Jan Lewis, John Sereno, Larry Greenwood, Steve Chance</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

|                |                                     |
|----------------|-------------------------------------|
| 06-27-12 17:26 | FYI: Ticket for XSS vulnerabilities |
|----------------|-------------------------------------|

|                                                                                                                                                                                                                                                                                                                                                                                                                          |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">Main</a>   <a href="#">My View</a>   <a href="#">View Issues</a>   <a href="#">Report Issue</a>   <a href="#">Change Log</a>   <a href="#">Roadmap</a>   <a href="#">Summary</a>   <a href="#">Docs</a>   <a href="#">Manage</a>   <a href="#">Edit News</a>   <a href="#">My Account</a>   <a href="#">Plugins</a>   <a href="#">Search</a>   <a href="#">Bugtracker Hierarchy</a>   <a href="#">Logout</a> |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

[Mantis 1.1.2](#)<sup>[^]</sup>  
Copyright © 2000 - 2008 Mantis Group  
[Mick.Ohrberg@noaa.gov](mailto:Mick.Ohrberg@noaa.gov)  
90 total queries executed.  
74 unique queries executed.

