

BlackBerry smartphones open to SMS attack

BlackBerry mobile devices are open to attack due to a certificate notification flaw in the smartphone's software, according to Research In Motion.

The problem lies in the BlackBerry Browser, specifically in the dialog box that alerts users if the URL they have clicked on does not match the domain they are being sent to, the company warned in an advisory.

To exploit the flaw, a hacker could craft a malicious website that spoofs a trusted website, then send users a link to that site using text messaging or email. If the malicious domain name contains a null character and the user chooses to access the site, the certificate-handling software on the device will note that there is a mismatch, but the warning dialog box will not display the null character in the link.

For example, the URL 'zd[null character]net.co.uk' will generate an alert, which will tell the user they are about to visit 'zdnet.co.uk'. BlackBerry users may ignore this alert, as malicious websites could appear benign, RIM said.

"RIM recommends that BlackBerry device users exercise caution when clicking on links that they receive in email or SMS messages," the company said in its advisory. "If a user visits a site that causes a BlackBerry Browser dialog box to warn the user about continuing the connection, the user should select Close connection."

BlackBerry Device Software from version 4.5 onwards is affected. RIM has provided a software update, available from the BlackBerry updates site, to mitigate the issue.

The [Private Investigator](#) agency Beowulf offers [undercover investigations](#) regarding mobile counter surveillance to determine whether an individual is being followed or investigated.