



June 2008 Update

Summary

Notable this month was the release of Mozilla Firefox 3.0, followed roughly five hours later by the private disclosure of a 0-day vulnerability affecting both version 3.0 and all 2.x versions.

Mass SQL injection attacks and Cross Site Scripting (XSS) vulnerabilities continue to be ongoing issues, with new incidents reported on near daily basis.

Trends and alerts

Firefox 3.0 was released by Mozilla on 18/06/08, and approximately five hours later a submission was made to the Zero Day initiative detailing the 0-day vulnerability affecting both the newly released Firefox 3.0 browser, along with older 2.0.x releases. Successful exploitation of the vulnerability could allow an attacker to execute arbitrary code on the client machine in the browser. They have verified the vulnerability and reported it privately to Mozilla. To successfully exploit this vulnerability user interaction is required, typically visiting a malicious website or clicking a link in an email. Although there are currently no known public exploits for this vulnerability, it does pose a security risk and users should be aware that Mozilla are yet to release a patch.

Mass SQL injection attacks continue to be a problem, affecting thousands of legitimate websites. The attacks use SQL injection to insert a script tag into a valid page, which then direct users to a fast flux domain which contains the malware. The attack typically comprises one single SQL statement, which will pull all the necessary information from the database, and set certain variables to return the script tag (and malicious domain), so that whenever the website uses a string from the database, the script tag is added. Database and website administrators may find the [Microsoft guide to protect against SQL injection](#) helpful to assess and secure the systems for which they are responsible.

Cross Site Scripting (XSS) attacks against both UK Government and local government websites continue to be prevalent, and GovCertUK would urge all web developers to properly sanitise any parts of a website that allows either user input or could allow a user to modify the output of any web application. Further details on XSS and mitigation can be found [here](#).

Microsoft released their [monthly security updates](#) covering Critical vulnerabilities in Internet Explorer, as well important patches for DirectX and Windows Bluetooth Stack.

Contact us

We welcome any queries about this report. Please contact us via one of the following means:

Email	enquiries@govcertuk.gov.uk
Telephone	01242 709311
Fax	01242 709113
Postal address	GovCertUK A2f P.O. Box 144 Cheltenham Gloucestershire GL51 0EX