



## July 2008 Update

### Summary

Security researchers hit the headlines in July, particularly on the subject of DNS implementation flaws and Mifare smartcard limitations. Many departments are likely to be susceptible to these vulnerabilities and should use the resources discussed below to evaluate exposure and implement fixes, if not already underway.

A great many websites continue to be affected by defacements, cross-site scripting attacks and the injection of malicious content. GovCertUK recommends following the advice available on the GovCertUK website and using CESG's comprehensive library of advice and best practice, including the IA Bookstore, to develop secure networks, websites and applications.

### Trends and alerts

It has been widely reported that a limitation in the current implementation of the Domain Name System (DNS) protocol makes it vulnerable to cache poisoning attacks. As technical details about the flaw and exploit code are now freely available, GovCertUK recommend that all organisations running a DNS server apply the appropriate patches at the earliest opportunity and ensure that any authoritative DNS servers referenced (e.g. ISP) have also been updated. The GovCertUK [advisory](#) has further details and SANS, among others, offers a good [summary of technical details](#).

Further work by Dutch researchers has proven that vulnerabilities in the Mifare Classic chip, used in some access control systems, can be exploited. A Dutch court ruling allows the researchers to publish their research in October; the GovCertUK [Mifare Advisory](#) provides additional details. GovCertUK advise all departments to review their security and access systems and take suitable action to secure systems and buildings prior to the publication of this research.

Reports released in July confirm the widespread infection of many legitimate websites with malicious software. A large number of these infections have been accomplished through SQL injection into a vulnerable website's database. GovCertUK remind webmasters to regularly audit websites for vulnerable code, to use safe coding techniques and to apply server and application patches as soon as testing has been completed.

In addition to the regular monthly updates Microsoft has released a [security advisory](#) relating to a vulnerability in the ActiveX control for the Snapshot Viewer for Microsoft Access. GovCertUK has published a [spot report](#) summarising the issue and mitigation advice and our review of patches released in the usual monthly cycle is available [here](#).

Research In Motion (RIM) has released a BlackBerry Enterprise Server (BES) security update to fix a vulnerability relating to how PDF files are processed via the Blackberry Attachment Service. Details of the issue, with links to the appropriate updates, are available from the [BlackBerry website](#).

## July news

The next GovCertUK training day is now arranged to be on Thursday 11<sup>th</sup> September 2008, held in London. We are planning to have two sessions, one in the morning and one in the afternoon, both following a similar agenda. This training is expected to be of more interest to IT managers; we hope to send out invitations in mid-August. If this training would be beneficial to you, please register your interest with GovCertUK enquiries.

In July GovCertUK hosted the second meeting of the year with a number of government departments and relevant trade associations to discuss phishing and e-crime issues. With the increase of Government services available online this issue is likely to affect more departments and governmental organisations in future. Those interested in attending the next meeting can contact us for further details.

Following the completion of the Data Handling Review and its outcomes, GovCertUK has published new [Incident Response Guidelines](#) outlining when and how to request our assistance with a computer security incident. Please contact us if unsure of the best course of action or if you are not able to evaluate the most appropriate classification for the incident.

## Contact us

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

Email	<a href="mailto:enquiries@govcertuk.gov.uk">enquiries@govcertuk.gov.uk</a>
Telephone	01242 709311
Fax	01242 709113
Postal address	GovCertUK A2f P.O. Box 144 Cheltenham Gloucestershire GL51 0EX