



March 2008 Update

Summary

March has seen a number of website defacements, cross-site scripting attacks and the continued injection of hidden crafted IFRAMEs to redirect the user to malicious websites or to download malware. CESG provides a comprehensive library of advice and best practice, including the IA Bookstore, – a valuable resource in minimising vulnerability exposure.

Many vendors, including Microsoft and VMware, released service packs and major security updates. GovCertUK recommend that all systems should be maintained to current patch levels wherever possible, after suitable testing.

Trends and alerts

A number of commercial companies and independent researchers have highlighted recent widespread hidden IFRAME injection and cross-site scripting (XSS) attacks on a number of popular websites. GovCertUK have published advice on [common XSS techniques and possible mitigations](#).

Following the release of the discovery of a security issue with Microsoft Vista BitLocker in February, Microsoft have summarised how to mitigate the effectiveness of this attack in a [Windows Vista Security blog posting](#). Exploitation appears to be only possible in limited circumstances.

It is common practice to use Adobe PDF documents to share information in a more reliable fashion. Some of the latest vulnerabilities in this format (see a [US-CERT summary](#)) accentuate the need to exercise caution when viewing a file (whether PDF or another document format) received from an unknown source. GovCertUK recommend the use of an up-to-date anti-virus program and for system administrators to consider constraining the permissible content of such files.

A number of software vendors have released important security updates this month and GovCertUK recommend that system administrators, after appropriate testing, apply the relevant patches to their environments wherever possible. This month's GovCertUK Summary of Microsoft Advisories is available for download at http://www.govcertuk.gov.uk/patch_advisories.shtml.

Following the long-anticipated release of the Microsoft Vista Service Pack GovCertUK has published an advisory on the impact of this update. Full details are available on the [GovCertUK website](#); a brief summary is to apply the patch after suitable testing.

An additional highlight this month is the recently released VMware update (see [VMware Security Advisory](#)) which, amongst other things, patches the host to guest shared folder directory traversal vulnerability. GovCertUK recommend applying this patch as soon as testing has been completed on your local computing environment.

March news

A successful and well-attended GovCertUK training day that took place in Cheltenham on 10th March covered the basics of incident response and included a number of technical briefings. We are planning another training day on Wednesday 10th September 2008; we expect to review some of the content of the March training day, with additional new material. Book it in your diary – invitations will be sent closer to the time.

The most recent WARP Operators Forum was hosted by GovCertUK, one of the best attended so far. The next WOF will be held in London on 2nd June 2008. Each WARP has a unique community focus; visit www.warp.gov.uk for further information, details on how to join or how to set up a new WARP.

GovCertUK would like to emphasise again the CESG Good Data Handling Guidance Information Pack, which brings together various advisories and Good Practice Guides. This can be found on the CESG IA Bookstore CD or the CESG GSi website. If not a GSi user or Bookstore recipient, please contact your local IT Security Officer or WARP administrator for further details.

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