



November 2007 Update

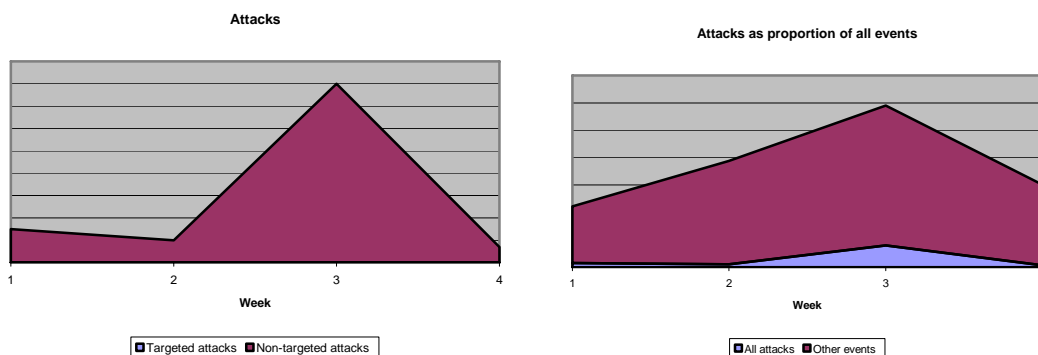
Summary

There have been many discussions in the national press about electronic attack against UK government computer networks. GovCertUK recommends all network administrators to continue following best practise guidelines regarding computer patching, monitoring, network security and user education. Watch out for new best practise whitepapers due to be published in the coming months.

The recent widely reported data loss from a government department highlights the need to safeguard the storage, handling and transfer of data within organisations and to other parties. GovCertUK to remind anyone submitting suspected attack material to follow procedures published on our website at <http://www.govcertuk.gov.uk/reporting-an-incident.shtml> or to use a secure, tracked delivery service.

Trends and alerts

We continued to see a fall in targeted attacks and total activity remained at a low level this month. On average 80% of all identified events remain web-based and not directly targeted to the receiving location. The graphs below give an indication of events logged in the past month:



Based on the analysis of network attack events GovCertUK has identified a number of currently patched vulnerabilities being exploited. We would particularly highlight the following Microsoft vulnerabilities:

GDI Vulnerability (security bulletin MS07-017)
Data Access Components Vulnerability (security bulletin MS07-009)
Vector Markup Language Vulnerability (security bulletin MS07-004)
XML Core Services Vulnerability (security bulletin MS06-071)
IE Cumulative Security Update (security bulletin MS06-067)
Windows Explorer Vulnerability (security bulletin MS06-057)
HTML Help Vulnerability (security bulletin MS06-046)
Windows Media Player Vulnerability (security bulletin MS06-024)
Data Access Components Function Vulnerability (security bulletin MS06-014)

Please refer to Microsoft security briefings
<http://www.microsoft.com/technet/security/current.aspx> for further information.

November news

GovCertUK is now releasing updates and alerts to WARP forum members via the GovXchange portal. For further details please contact your local WARP operator, who should be able to gain access on your behalf.

Our updated Google Search Application XSS Vulnerability report has been published, noting details of the recently released patch. This briefing can be downloaded from the website at <http://www.govcertuk.gov.uk/alerts.shtml>.

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