



12/11/07

GovCertUK Summary - October

Signatures and 'Black lists'

GovCertUK periodically release signatures and lists of domains or IP addresses that have been associated with malicious content. This is for use by Government departments or their service providers for detecting possible malicious activity.

These signatures are generated through analysis that GovCertUK performs or from information provided by other parties. Readers are reminded that some of these signature lists carry handling instructions that must be followed.

If you wish to receive these lists, please contact GovCertUK using the details provided below.

Detected Attacks

The 85% of attacks that GovCertUK identify remain web based and non-targeted. These come from either redirects from compromised legitimate web sites, hidden IFRAMES or browsing non-work related web sites.

The vulnerabilities exploited are numerous and include MS07-017 (ANI files), MS07-009 (Adodb.Connection), MS06-014 (RDS.Dataspace), MS06-071 (XMLHTTP) and MS06-057 (WebViewFolderIcon). A regular patching policy, and user education combined with detailed content filtering will help mitigate this threat.

Targeted email attacks also continue to be detected. Regular patching will also help mitigate this threat; however user education remains fundamental to mitigating this threat.

XSS Guidance and Technical Papers

GovCertUK have published guidance on mitigating Cross-Site Scripting (XSS) vulnerabilities. This can be found on the GovCertUK website at <http://www.govcertuk.gov.uk/technical-papers.shtml>

GovCertUK aim to produce further technical papers on topics of interest, and these will be published to the same location.

Brief Summary - September

General

If you have any questions about this report, please contact us at:

enquiries@govcertuk.gov.uk

If you need to report an incident to GovCertUK, please follow the guidance at www.govcertuk.gov.uk/reporting.shtml