

GovCertUK

Summary 01/02/07 – 26/02/07

Introduction

GovCertUK aim to provide regular updates on recent activity and publications which might be of interest to its constituency. It is impossible to cover all operating systems and applications, however we hope to cover the major topics. Please feel free to respond with ideas or comments.

Recent vulnerabilities and patches

02/02/07 Microsoft published details of a remote code execution vulnerability at <http://www.microsoft.com/technet/security/advisory/932553.msp> affecting Office 2000, XP and 2003. Currently only Excel has been targetted, however it is expected that other Office components will be exploited shortly.

05/02/07 Samba 3.0.24 was released which fixes CVE's 2007-0452, 2007-0453 and 2007-0454.

08/02/07 PHP released version 5.2.1 which "is a major stability and security enhancement of the 5.X branch".

12/02/07 Sun released update 11 for Java 1.5.0, which includes a number of bug fixes.

13/02/07 Microsoft released details of 12 patches as part of their regular patch cycle. These included 6 critical and 6 important patches. Check for relevant patches and install them once fully tested against your infrastructure.

13/02/07 Cisco released details of vulnerabilities in IOS IPS (Intrusion Prevention System). Those running affected versions (12.x) should check the Cisco website for workarounds and downloads.

15/02/07 Cisco released details of multiple vulnerabilities in Cisco PIX and ASA appliances. The affected products include the PIX 500 Series Security Appliances, and the ASA 5500 Services Adaptive Security Appliances.

15/02/07 Apple released a security update for Mac OS X and v10.3.9 and v10.4.8. Users of versions should check the apple website for advice and downloads.

19/02/07 SourceFire announced a buffer overflow vulnerability in the DCE/RPC preprocessor in Snort versions 2.6.1, 2.6.1.1, 2.6.1.2 and 2.7.0 beta 1. Users of versions 2.6.1.x should upgrade to 2.6.1.3, whilst 2.7.0 beta users should disable the affected preprocessor.

23/02/07 Mozilla released version 2.0.0.2 of Firefox that fixes seven security issues. Anyone running older versions of Firefox should install this update once they are happy that it does not adversely impact their local configuration.

Articles of interest

The US NIST (National Institute of Standards and Technology) released 3 new documents on 21/02/07:

1. SP 800-45 Version 2, [Guidelines on Electronic Mail Security](#)
2. SP 800-94, [Guide to Intrusion Detection and Prevention Systems \(IDPS\)](#)
3. SP 800-97, [Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i](#)

Activity of interest

06/02/07 Various articles were released detailing distributed denial of service (DdoS) attacks on the root DNS servers. It was reported that up to three of these servers were overwhelmed, however this went largely unnoticed within the UK and should now be fully resolved.

09/02/07 GovCertUK published an alert on 9th February detailing a phishing attack claiming to be from HM Revenue and Customs. The content of the email attempts to entice the user to click on a link to claim a tax refund that is due. The examples available to GovCertUK used various sites, which we have been working to take down.

Since this time we have detected a number of other phishing emails, containing links to fraudulent sites and asking for user details. It is important to remind all users of the dangers of this type of attack.

Other news

01/02/07 GovCertUK went operational from the 1st February 2007 to provide a computer emergency/response team for HM Government. GovCertUK is a part of CESG (the Communications and Electronic Security Group), which as the National Technical authority for Information Assurance (IA) has assumed the lead role within Government for IA advice.

Contact Us:

Telephone:	01242 709311
Fax:	01242 709113
General Enquiries:	enquiries@govcertuk.gov.uk
Incidents and Alerts:	incidents@govcertuk.gov.uk
Restricted communications (GSI only):	govcertuk@cesg.gsi.gov.uk
website:	www.govcertuk.gov.uk