



DNS Exploit – Updated 25-Jul-08

Public disclosure of DNS exploit

There is a publically known flaw with the implementation of DNS. The actual exploit details of this flaw are going to be made public at the Black Hat Conference in August this year. Public discussion of the exploit is now more widespread, including speculation on the details of the exploit. However there is no evidence of exploit code being released as yet.

Software vendors have issued patches that will mitigate against this flaw being exploited. The standard GovCertUK policy of software patching applies and it is highly recommended that the patch is applied to vulnerable systems as soon as possible. Good network security management can also aid in the defence against this exploit.

Update 25th July 2008

Technical details of this vulnerability and exploit code are now publicly available for download. This makes it trivial for an attacker to compromise vulnerable DNS implementations.

Whilst patches are available, it has been reported that the network architecture can impair their effectiveness. Explicit examples where this has been reported are where the DNS server is behind Network Address Translation (NAT) or Port Address Translation (PAT) devices. In these circumstances departments are advised to contact their providers.

GovCertUK recommend that those departments with publicly accessible DNS servers should check with their service providers or DNS vendor for available patches and mitigation advice.

All DNS servers should have patches applied as soon as testing is complete.

CESG, as the National Technical Authority for Information Assurance (IA), has the lead responsibility within Government for providing Information Assurance advice to public sector organisations.

GovCertUK is responsible for Computer Security Incident Response within UK Government, and provides an emergency response capability to public sector organisations that may require technical support and advice during periods of electronic attack or other network security incidents.

GovCertUK provides an email notification service intended for UK Government departments, providing news, security alerts and relevant technical bulletins. You will need to register with a valid UK government email address, and you must be either the Information Technology Security Officer (ITSO) or Computer Security Incident Response Officer (CSIRO) for your department, or provide delegated authority from them.

The CESG GovCertUK Incident Response team provides 24 hours a day, 7 days a week operation and can be contacted by the following methods:

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