



Issued: 08/08/2008

---

## Reports of SQL injection attack on .gov.uk sites

---

Recent press coverage<sup>1</sup> has suggested that almost 3000 gov.uk sites have been compromised as part of a wide scale SQL Injection attack known as ASPROX. GovCertUK have been monitoring these attacks for a number of weeks, and working with affected departments in order to clean any infected websites.

Analysis contained within the reports relies on using Google to search for websites containing the hallmarks of the ASPROX attack. It should be noted that the vast majority of gov.uk pages returned by the Google search are cached results, and have been cleaned since last being scanned by Google. This gives a false impression of the current position.

Webmasters concerned that they may have been compromised by the ASPROX attack can search across their site for the following strings:

- ngg.js
- js.js
- b.js

Presence of these strings may indicate a successful SQL injection. GovCertUK can be contacted to assist with mitigation and remediation advice in this instance.

---

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.

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:	<a href="mailto:enquiries@govcertuk.gov.uk">enquiries@govcertuk.gov.uk</a>
Incidents & Alerts:	<a href="mailto:incidents@govcertuk.gov.uk">incidents@govcertuk.gov.uk</a>
Restricted communications (GSI only):	<a href="mailto:govcertuk@cesg.gsi.gov.uk">govcertuk@cesg.gsi.gov.uk</a>
Website:	<a href="http://www.govcertuk.gov.uk">www.govcertuk.gov.uk</a>

---

<sup>1</sup> SANS Incident Handlers Diary (<http://isc.sans.org/diary.html?storyid=4840>)  
The Register ([http://www.theregister.co.uk/2008/08/07/new\\_sql\\_attacks/](http://www.theregister.co.uk/2008/08/07/new_sql_attacks/))