



Australian Government

Attorney-General's Department



AUSTRALIA'S NATIONAL
COMPUTER EMERGENCY RESPONSE TEAM

CERT Australia Industry News

Another round of mass SQL injection attacks

Cyber criminals are currently exploiting poorly written .net code in order to inject malicious commands into websites. Users running Microsoft IIS or SQL Server should check that their databases have not been compromised as part of this attack.

Technical details

Through the use of obfuscated SQL commands, attackers are injecting malicious JavaScript into every text field within vulnerable databases. When your website is viewed in a browser with JavaScript enabled, the code will execute and make a request to a malicious site in order to retrieve further instructions.

Historically the requests retrieve malware which can then take full control of the client system providing it can run with administrative privileges. These compromised machines often then become part of a Botnet as was seen in the Asprox attacks back in 2008 [1], which are then used to compromise further sites.

Several vendors have written up detailed analysis reports on this and similar attacks. [2,3]

Business impact

The aim of this SQL injection attack is to make use of legitimate sites in order to spread malware. There is a higher level of success in these attacks due to the trusted nature of the websites involved.

If your site is utilising a database that has been compromised, you may be serving malware to current or potential customers. This can result in a loss of business or trust and can also lead to your site being blacklisted by search engines.

Further reading

[1] <http://www.zdnet.com/blog/security/fast-fluxing-sql-injection-attacks-executed-from-the-asprox-botnet/1122>

[2] <http://isc.sans.edu/diary.html?date=2010-08-15>

[3] <http://www.f-secure.com/weblog/archives/00001427.html>

This document remains the property of the Australian Government. The information contained in this document is for the use of the intended recipient only and may contain confidential or privileged information. If this document has been received in error, that error does not constitute a waiver of any confidentiality, privilege or copyright in respect of this document or the information it contains.

The material and information in this document is general information only and is not intended to be advice. The material and information is not adapted to any particular person's circumstances and therefore cannot be relied upon to be of assistance in any particular case. You should base any action you take exclusively on your own methodologies, assessments and judgement, after seeking specific advice from such relevant experts and advisers as you consider necessary or desirable. To the extent permitted by law, the Australian Government has no liability to you in respect of damage that you might suffer that is directly or indirectly related to this document, no matter how arising (including as a result of negligence).