empath-e
MAKING CRM MAKE **SENSE**

Tech Bulletin
2nd March 2016
Updated:

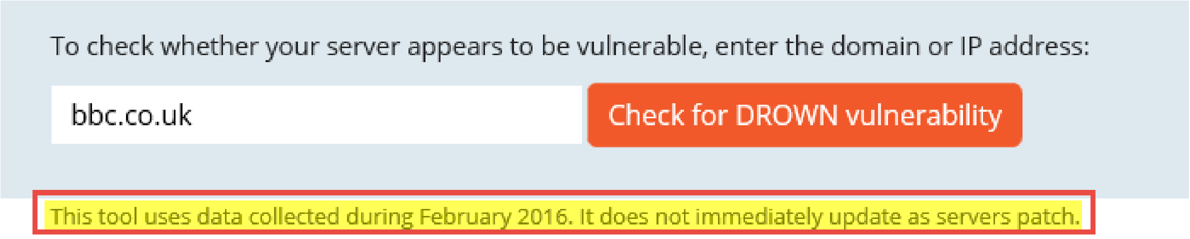
www.empath-e.com/support

Issue

A report, highlighted on the BBC website http://www.bbc.co.uk/news/technology-35706730 may have caught your eye. This relates to the *"Thousands of popular sites' at risk of Drown hack attacks"* issue that is current. Drown is an acronym for "Decrypting the Rivest-Shamir-Adleman (RSA) algorithm with Obsolete and Weakened eNcryption".

Reason

It should be noted that, like the Year 2000 bug, whilst this is a very valid concern - and one that should be addressed, it is also evident that the checking tools provided are, in themselves, open to fault. You can check your domain using https://drownattack.com/#check But, it should be noted from their own website as:

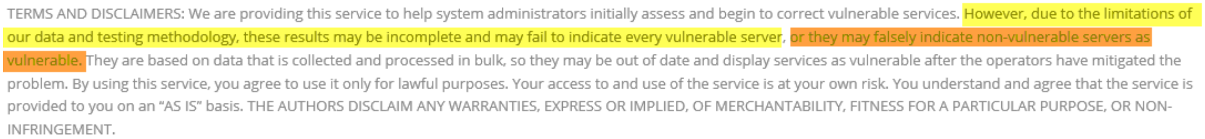


To check whether your server appears to be vulnerable, enter the domain or IP address:

bbc.co.uk

This tool uses data collected during February 2016. It does not immediately update as servers patch.

Which, as you can see, means they have tested and cached results from millions of domains and any subsequent fixes would still result in **false positives.** Further, the test cannot distinguish between sites that have an issue and an SSL certificate shared amongst servers where an issue doesn't exist:



TERMS AND DISCLAIMERS: We are providing this service to help system administrators initially assess and begin to correct vulnerable services. However, due to the limitations of our data and testing methodology, these results may be incomplete and may fail to indicate every vulnerable server, or they may falsely indicate non-vulnerable servers as vulnerable. They are based on data that is collected and processed in bulk, so they may be out of date and display services as vulnerable after the operators have mitigated the problem. By using this service, you agree to use it only for lawful purposes. Your access to and use of the service is at your own risk. You understand and agree that the service is provided to you on an "AS IS" basis. THE AUTHORS DISCLAIM ANY WARRANTIES, EXPRESS OR IMPLIED, OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT.

For this reason we acknowledge the issue but feel that the test suites, due to their own vulnerabilities, are – at worst - scare-mongering and will create angst to businesses where none need exist. If you feel your site could be exposed we can check this using other tools as required.

UPDATE: 04/03/2016 – They appear to have acknowledged this short-coming and the site now allows for a re-check of each domain. This enables an admin to fix the issue and verify it is fixed.

There are three concerns that affect our customer base:

OpenSSL – where used (only with VMWare v5.5 or earlier), these have already been patched
Microsoft IIS – we only have customers using IIS v7 and above and none are set to use SSLv2
Symantec Mail Gateway – this requires updating to version 10.6.7 to comply with DROWN – this is an active task, expected to be complete by end of March 2016.

You will probably find that your site is listed as vulnerable – simply because the tool is unable to distinguish the shared SSL certifcate in use and the servers the other side and simply marks it as a problem. This is a false positive.

It is unknown as to whether the publishers will update their cache & data collected – which rather makes the use of the test site unworkable and more useless over time if it is not further updated.

UPDATE: 04/03/2016 – They appear to have acknowledged this short-coming and the site now allows for a re-check of each domain. This enables an admin to fix the issue and verify it is fixed.

Resolution

Hundreds of security issues are found each day and reported to CVE but this does not necessarily mean that you will be affected. The results of DROWN show that many major sites (such as BBC, Microsoft, Yahoo, Weibo, Alibaba) are exposed to this issue so potential attackers are most likely to go after these sites first.

At the time of writing [the report] – it is not believed any sites had been attacked, using this mechanism, prior to disclosure of the issue.

Whilst it may have been prudent by the authors to publish their report, it could also be said that in doing so all they have done is highlight to the hacking world a non-issue for many and published an open-threat to be targeted and, therefore, only propagated an issue best resolved by vendors.

There is also the not-so-small issue that, should they use Amazon EC2, it would cost an attacker £314 per site in compute time to perform the attack – which only further concretes the idea that smaller sites would remain unaffected – giving plenty of time to fix the issue, should it exist, for you.