JUNE 2015

blackfoot

BLACKFOOT NEWSFLASH

ENCRYPTION FLAW EXPOSES SECURE WEBSITES TO LOGJAM ATTACK

Following the publication of the PCI DSS v3.1 in April 2015, outlawing the use of SSL or early versions of TLS, another TLS vulnerability came to light in mid-May 2015.

LogJam has two potential attacks:

Exploiting a weakness in the TLS protocol to conduct a man-in-the-middle attack and downgrade the TLS connection to 512-bit encryption

Exploiting the weakness of using commonly-used, known prime numbers, or those less than 2048-bit in length (2 to the power of 2048 possible combinations)

Around 8% of the top one million HTTPS sites are believed to be affected, allowing attackers to compromise encrypted communications, and giving users false assurance as to the security of such websites.

What is the threat?

Vulnerabilities in TLS could be used by attackers to compromise encrypted communications for criminal gain, electronic surveillance and so on.

The Diffie-Hellman key exchange is a widespread cryptographic algorithm and fundamental to many protocols, including HTTPS, SSH, IPsec, SMTPS and those relying on TLS. It allows two parties to agree on a shared encryption key over an untrusted, unencrypted network, such as the internet.

Millions of servers all use the same prime numbers for Diffie-Hellman key exchange. This was believed to be safe as long as new key exchange messages were generated for every connection. However, the most efficient algorithm for breaking a Diffie-Hellman connection is dependent only on knowing this prime number, after which an attacker can quickly break individual connections.

The authors of the LogJam Attack paper — a team of academics and Microsoft researchers — cracked the most commonly used 512-bit primes for TLS, meaning that the LogJam attack can be used to downgrade around 80% of TLS servers supporting the DHE_EXPORT.

As to the long-term security of Diffie-Hellman key exchange, the authors contend that due to the time, resource and compute power necessary, an academic team could break a 768-bit prime and a nation state a 1024-bit prime.

What is the potential impact?

Websites, mail servers and other TLS-dependent services that support DHE_EXPORT keys are vulnerable to the LogJam attack. Estimates of the vulnerabilities are as follows:

HTTPS — Top one million domains	8.4%
HTTPS — Browser-trusted sites	3.4%
SMTP+StartTLS — IPv4 Address Space	14.8%
POP3S — IPv4 Address Space	8.9%
IMAPS — IPv4 Address Space	8.4%

How to tell if you are affected or vulnerable

A server test is available at **https://weakdh.org/sysadmin.html** which will test any website for LogJam but also many other known web server vulnerabilities.

Server administrators can also verify the web server configuration to ensure that all ciphers now known to be insecure are disabled.

Next steps

If you run a web or mail server:

- **Disable support for weaker encryption methods, such as 512-bit**
- **Upgrade your server to stronger encryption methods, such as 2048-bit**
- **Regenerate your server's Diffie-Hellman primes regularly and do not hard-code standard primes into TLS cryptographic libraries**
- **Consider moving to Elliptic-Curve Diffie-Hellman (ECDH) which does not rely on prime numbers and is less susceptible to attack**

If you use a browser, ensure you have the most recent version of your browser installed and check for updates regularly. Google Chrome (including Android Browser), Mozilla Firefox, Microsoft Internet Explorer and Apple Safari are all deploying fixes for the LogJam attack.

Blackfoot statement of opinion

The LogJam vulnerability is a legacy of the US export restrictions on cryptographic tools of the 1990s. This limited the complexity of the encryption on such software to 512-bit. The export restrictions were later relaxed and stronger encryption methods deployed.

There is a possible but small impact that fixing this vulnerability may prevent legacy operating systems from working. It is good business practice to conduct due diligence before making changes, however unlikely it is that client browsers are only capable of using 512-bit encryption.

Further reading

The LogJam Attack - **https://weakdh.org**

For more information

Should you require further support, please contact your Blackfoot representative, call 0845 805 2409 or **e-mail info@blackfootuk.com**

blackfoot

Blackfoot UK Limited
Tel: 0845 805 2409
E-mail: info@blackfootuk.com
Web: www.blackfootuk.com

ADVISE >

ASSESS >

ASSURE >

This material is for information purposes only and does not take into consideration the particular circumstances or objectives of your business. Whilst every reasonable effort has been made to ensure the accuracy of the information in this document, Blackfoot UK Limited shall not be held liable for any errors or omissions.