Logjam Attack: No Risk for ViPNet VPN Encryption

Berlin, June 8, 2015 – Thousands of mail, web, SSH, and VPN servers are vulnerable to a new attack (called Logjam) that affects Diffie-Hellman key exchange. The Internet key exchange (IKE) protocol that uses the Diffie-Hellman algorithm is widely implemented in data encryption (for example, by SSL/TLS). ViPNet technology by Infotecs is essentially resistant to man-in-the-middle attacks. ViPNet does not use the IKE, because secure ViPNet communication does not require exchanging keys over the Internet.

On May 20, 2015, a team of several security researchers from US announced a weakness in Diffie-Hellman key exchange exploited by so-called "Logjam attack". The weakness is caused by a fault in TLS protocol that is used for HTTP, SSH, and VPN connection encryption. It can be exploited by man-in-the-middle attacks (MITM). Cyber criminals can monitor or even manipulate the data traffic between two or more communication parties. The actual weakness is in the TLS handshake procedure, during which the attacker offers insecure export key exchange instead of the normal Diffie-Hellman key exchange. In response the server continues exchanging insecure but valid 512-bit key. According to the security researches, since cyber criminals have precalculated discrete logarithms, an attack can happen within minutes [1] [2] [3].

Generally, the Logjam attack puts at risk all encryption methods that use Diffie-Hellman algorithm and key exchange over the Internet (IKE). As already mentioned, these include the TLS protocol and its predecessor SSL that are widely used for SSH, mail, web, and VPN connection encryption.

The ViPNet VPN encryption solution by Infotecs is not affected by the Logjam attack. ViPNet does not require exchanging keys using Diffie-Hellman algorithm. All initial keys will be distributed and installed on the clients once and immediately during their deployment. As a result, all clients have the relevant keys before the connection between them can be established. Thus, the clients do not need to exchange keys once again right before the data exchange with each other. ViPNet VPN uses symmetric key management that is considered to be highly secure and is used by the military. MITM attacks against ViPNet technology are essentially impossible. Cyber criminals cannot exploit key exchange over the Internet, because it is not used to provide secure communication.

Furthermore, every IP packet in a ViPNet network is encrypted using a derivative of a key. Even if an attacker intercepts and analyses an IP packet, it will be completely ineffective, because any other IP packet is encrypted using another key.

You can download a trial version of ViPNet VPN security solution (allows you to create 2 coordinators and 10 clients) at www.infotecs.biz/download/.

Further information

[1] Background information about Logjam attack from WeakDH.org (Logjam discoverers, group of computer scientists), 20.05.2015
https://weakdh.org/

[2] „Logjam security flaw leaves top HTTPS websites, mail servers vulnerable", ZDNet.com, 20.05.2015
http://www.zdnet.com/article/logjam-security-flaw-leaves-tens-of-thousands-of-https-websites-vulnerable/

[3] „Logjam-Angriff: Schwäche im TLS-Verfahren gefährdet Zehntausende Webseiten", Golem.de, 20.05.2015
http://www.golem.de/news/logjam-angriff-schwaeche-im-tls-verfahren-gefaehrdet-zehtausende-webseiten-1505-114161.html

About Infotecs

Infotecs has provided advanced network communications, information security software and hardware solutions since 1991. A pioneer of software-based VPN solutions, Infotecs developed its next generation ViPNet technology to deliver greater security, flexibility, and throughput than IPSec and other standard-based VPN products. ViPNet is the only VPN solution that supports true end-to-end, client-to-client security, and is unique in offering secure peer-to-peer communications. More than 1,000,000 clients, offices, and servers have been securely connected with ViPNet products backed up by an unparalleled world-class support, development, and technical team. Our solutions are designed to solve the toughest security challenges by providing superior protection that is flexible and effective. Additional information on the company is available at visit: www.infotecs.biz.

Contact

Infotecs GmbH
Anja Mueller
Marketing & Communications
Oberwallstr. 24
10117 Berlin, Germany
Phone: +49 30 206 43 66-52
Fax: +49 30 206 43 66-66
anja.mueller@infotecs.biz

Twitter: twitter.com/InfotecsEnglish
Facebook: www.facebook.com/pages/Infotecs-Gmbh_english/400720220013566