Logjam-Attacke: Verschlüsselung mit ViPNet VPN nicht betroffen

Berlin, 02. Juni 2015 – Durch einen neuen Angriff (genannt Logjam) auf den Diffie-Hellman-Schlüsselaustausch sind aktuell unzählige Mail-, Web-, SSH- und VPN-Server unsicher. Verfahren mit Internet Key Exchange (IKE), welche den Diffie-Hellman-Schlüsselaustausch verwenden, werden sehr häufig zur Verschlüsselung (z. B. bei SSL/TLS) eingesetzt. Bei der ViPNet Technologie von Infotecs sind Man-in-the-Middle-Angriffe grundsätzlich nicht möglich. Der Schlüsselaustausch (IKE) kann bei ViPNet nicht ausgenutzt werden, da kein öffentlicher Schlüsselaustausch über das Internet notwendig ist, um eine sichere Kommunikation zu gewährleisten.

Am 20. Mai 2015 veröffentlichte ein Team aus mehreren US-Sicherheitsforschern eine Schwachstelle im Diffie-Hellman-Schlüsselaustausch, genannt Logjam-Attacke. Logjam beruht auf einem Fehler im TLS-Protokoll, welches zur Verschlüsselung von HTTPS-, SSH- sowie VPN-Verbindungen genutzt wird. Durch diese Sicherheitslücke werden Man-in-the-Middle-Angriffe (MITM) möglich. Cyberkriminelle können den Datenverkehr zwischen zwei oder mehreren Kommunikationspartnern einsehen und im schlimmsten Fall manipulieren. Die eigentliche Schwachstelle liegt im TLS-Handshake, bei welchem der Angreifer der Gegenstelle einen unsicheren Export-Schlüsselaustausch anstatt des üblichen Diffie-Hellman-Schlüsselaustauschs anbietet. Als Rückmeldung des Servers folgt ein als sehr unsicher geltender 512-Bit-Schlüsselaustausch. Indem Cyberkriminelle bereits im Vorfeld Berechnungen zu diskreten Logarithmen durchführen, wird laut den Sicherheitsforschern ein Angriff in Echtzeit innerhalb von Minuten möglich [1] [2] [3].

Gefährdet durch die Logjam-Attacke sind prinzipiell alle Verschlüsselungsverfahren, welche auf dem Diffie-Hellman-Verfahren beruhen und bei welchen ein öffentlicher Schlüsselaustausch über das Internet (IKE) stattfindet. Dazu zählen wie bereits erwähnt das TLS-Protokoll, sowie der Vorgänger SSL, welche häufig zur Verschlüsselung von SSH-, Mail-, Web- sowie VPN-Verbindungen eingesetzt wird.

Die Verschlüsselungslösung ViPNet VPN von Infotecs bleibt von der Logjam-Attacke unberührt. Ein Schlüsselaustausch im Sinne von Diffie-Hellman findet nicht statt. Alle initialen Schlüssel werden einmalig und bereits beim Rollout auf die verschiedenen Clients verteilt und installiert. Das bedeutet, dass alle Teilnehmer bereits vorab die entsprechenden Schlüssel besitzen, noch bevor überhaupt eine Verbindung zu anderen Teilnehmern aufgebaut werden kann. Unmittelbar vor der Kommunikation bzw. dem Datenaustausch zwischen den Clients erfolgt kein erneuter Schlüsselaustausch. ViPNet VPN arbeitet mit einem symmetrischen Schlüsselmanagement, welches als hochsicher gilt und auch im militärischen Bereich eingesetzt wird. MITM-Attacken bleiben bei der ViPNet Technologie grundsätzlich erfolglos. Um eine sichere Kommunikation zu gewährleisten, ist ein öffentlicher Schlüsselaustausch über das Internet nicht notwendig. Demzufolge kann dieser auch nicht von Cyberkriminellen ausgenutzt werden.

Darüber hinaus verschlüsseln die IT-Sicherheitsexperten von Infotecs jedes einzelne IP-Paket mit einer Ableitung des Austauschschlüssels. Würde ein Angreifer ein IP-Paket abfangen und analysieren, wäre dies weniger zielführend, da jedes andere IP-Paket auch mit einem anderen Schlüssel kodiert wird.

Die Security-Lösung ViPNet VPN kann unter www.infotecs.de/download/ als Testversion (beinhaltet 2 Coordinatoren und 10 Clients) heruntergeladen werden. IT-Verantwortliche, welche nähere Details zum Thema symmetrische Verschlüsselung und ViPNet VPN erfahren möchten, können unter www.infotecs.de/whitepaper/ die kostenfreien Whitepapers anfordern.

Weiterführende Informationen

[1] Hintergrundinformationen zur Logjam-Attacke von WeakDH.org (Logjam-Entdecker, Team von US-Sicherheitsforschern), 20.05.2015
https://weakdh.org/

[2] „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

[3] „Logjam-Attacke: Verschlüsselung von zehntausenden Servern gefährdet", heise Security, 20.05.2015
http://www.heise.de/security/meldung/Logjam-Attacke-Verschluesselung-von-zehntausenden-Servern-gefaehrdet-2657502.html

Über Infotecs

Seit 1991 stellt Infotecs innovative Netzwerk-Kommunikations- sowie IT-Sicherheitslösungen als Soft- und Hardware zur Verfügung. Als erfahrener Spezialist software-basierter VPN-Lösungen entwickelte Infotecs die ViPNet Technologie, um mehr Sicherheit, Flexibilität und Effizienz als IPSec oder andere standardbasierte VPN-Produkte bieten zu können. Als einzige VPN-Lösung unterstützt ViPNet echte Punkt-zu-Punkt-Verbindungen. Mehr als 1.000.000 Endgeräte, Firmenstandorte und Server konnten bisher mithilfe von ViPNet sicher miteinander verbunden werden – unterstützt durch ein erstklassiges IT-Entwicklungs- und Support-Team. Unsere Lösungen wurden für die härtesten Anforderungen an die IT-Sicherheit der „Next Generation" konzipiert und bieten zuverlässigen, flexiblen sowie effektiven Schutz. Weitere Informationen zum Unternehmen finden Sie unter www.infotecs.de.

Kontakt

Infotecs GmbH
Anja Müller
Marketing & Kommunikation
Oberwallstr. 24
D-10117 Berlin
Tel.: +49 30 206 43 66-52
Fax: +49 30 206 43 66-66
anja.mueller@infotecs.de

Twitter: twitter.com/InfotecsDeutsch
Facebook: www.facebook.com/InfotecsGmbH
Xing: www.xing.com/companies/infotecsinternetsecuritysoftwaregmbh
Google+: plus.google.com/+InfotecsDe/
LinkedIn: www.linkedin.com/company/infotecs-internet-security-software-gmbh