idw - Informationsdienst Wissenschaft
Nachrichten, Termine, Experten

Press release

Ruhr-Universität Bochum
Dr. Julia Weiler

08/14/2018
http://idw-online.de/en/news700594

Research results
Information technology
transregional, national

Sicherheitslücken im Internetprotokoll „IPsec“ identifiziert

Forscher des Horst-Görtz-Instituts für IT-Sicherheit (HGI) an der Ruhr-Universität Bochum (RUB) haben in Zusammenarbeit mit Wissenschaftlern der polnischen Universität Opole nachgewiesen, dass das Internetprotokoll „IPsec“ angreifbar ist. Das in der Protokollfamilie enthaltene Internet-Key-Exchange-Protokoll „IKEv1“ birgt Sicherheitslücken, die es Angreifern potenziell ermöglichen, sich in einen Kommunikationsprozess zwischenzuschalten und gezielt Informationen abzugreifen.

Die Forschungsergebnisse veröffentlichen Dennis Felsch, Martin Grothe und Prof. Dr. Jörg Schwenk vom Lehrstuhl für Netz- und Datensicherheit der RUB sowie Adam Czubak und Marcin Szymanek von der Universität Opole am 16. August 2018 auf der Usenix Security Konferenz sowie in ihrem Blog (https://web-in-security.blogspot.com/).

Sichere und verschlüsselte Kommunikation

Als Weiterentwicklung des Internetprotokolls (IP) zielt „IPsec“ darauf ab, mittels Verschlüsselungs- und Authentifizierungsmechanismen einen kryptografisch sicheren Kommunikationsablauf über öffentlich zugängliche beziehungsweise unsichere Netze, wie das Internet, zu ermöglichen. Diese Form der Kommunikation ist mitunter für Unternehmen von Bedeutung, deren Mitarbeiter dezentral arbeiten – etwa im Außendienst oder am Heimarbeitsplatz – und dennoch auf Unternehmensressourcen zugreifen müssen. Das Protokoll kann zudem für den Aufbau von virtuellen privaten Netzwerken, kurz VPN, genutzt werden.

Um mit „IPsec“ eine verschlüsselte Verbindung herstellen zu können, müssen sich beide Parteien vorher authentifizieren und Schlüssel für die gemeinsame Kommunikation definieren. Die automatische Schlüsselverwaltung ebenso wie die Authentifizierung, beispielsweise durch Passwörter oder digitale Signaturen, erfolgt über das Internet-Key-Exchange-Protokoll „IKEv1“. „Auch wenn das Protokoll bereits als veraltet gilt und mit IKEv2 längst eine neuere Version auf dem Markt verfügbar ist, zeigt die Praxis, dass es immer noch in Betriebssysteme implementiert wird und sich nach wie vor großer Beliebtheit erfreut, auch in neueren Geräten,“ erklärt Dennis Felsch. Doch genau dieses Protokoll birgt Schwachstellen, wie die Forscher bei ihrem Angriff herausfanden.

Bleichenbacher-Angriff erfolgreich

Dabei griffen die Wissenschaftler im Rahmen ihrer Forschung den verschlüsselungsbasierten Anmeldemodus von „IPsec“ mithilfe des sogenannten Bleichenbacher-Angriffs an, der erstmals 1998 angewendet wurde. Das Prinzip: Eine verschlüsselte Nachricht wird gezielt mit Fehlern versehen und vielfach an einen Server verschickt. Die Antworten des Servers auf die fehlerhafte Nachricht lassen nach und nach immer mehr Rückschlüsse auf den verschlüsselten Inhalt zu. „Man nähert sich dem Ergebnis auf diese Weise quasi Schritt für Schritt, bis man am Ziel ist,“ sagt Martin Grothe und ergänzt: „Es ist wie ein Tunnel mit zwei Endpunkten. Es reicht aus, wenn eine der beiden Parteien verwundbar ist. Letztlich ermöglicht es die Schwachstelle dann, dass ein Angreifer in den Kommunikationsprozess eingreifen, die Identität eines der Kommunikationspartner übernehmen und so aktiv Datendiebstahl betreiben kann.“

Bei der Hardware von vier Netzwerkausrüstern war der Bleichenbacher-Angriff erfolgreich. Betroffen waren Clavister, Zyxel, Cisco und Huawei. Die Hersteller wurden bereits informiert und haben die Sicherheitsmängel behoben.

Passwörter im Visier

Neben dem verschlüsselungsbasierten Anmeldemodus haben die Forscher auch die passwortbasierte Anmeldung unter die Lupe genommen. „Die Authentifizierung über Passwörter erfolgt mit Hashwerten, ähnlich einem Fingerabdruck. Dabei konnten wir bei unserem Angriff zeigen, dass IKEv1 ebenso wie das aktuelle IKEv2 hier Schwachstellen offenbaren und angreifbar sind – insbesondere wenn das Passwort schwach ist. Ein sehr komplexes Passwort ist daher der beste Schutz bei Verwendung von IPsec in diesem Modus," resümiert Martin Grothe. Über die Sicherheitslücke wurde auch das Computer Emergency Response Team (CERT) informiert, das als Koordinator bei der Lösung von konkreten IT-Sicherheitsvorfällen fungiert und die Forscher bei der Bekanntgabe der Sicherheitslücke unterstützte.

Entwarnung für Anwender und Netzwerkausrüster

Bei der identifizierten Bleichenbacher-Schwachstelle handelt es sich nicht um einen Fehler im Standard, sondern um einen Implementierungsfehler, der vermeidbar ist – es kommt also darauf an, wie die Hersteller das Protokoll in ihre Geräte einbinden. Zudem muss sich der Angreifer erst innerhalb des Netzwerks befinden, um aktiv werden zu können. Dennoch zeigt der erfolgreiche Angriff der Forscher, dass etablierte Protokolle wie „IPsec" nach wie vor die Bleichenbacher-Lücke enthalten und damit angreifbar sein können.

Ergebnispräsentation auf Konferenz

Das Forscherteam um Jörg Schwenk wird die Schwachstellen beim Usenix Security Symposium präsentieren, das vom 15. bis zum 17. August 2018 in Baltimore, USA, stattfindet.

contact for scientific information:

Dennis Felsch
Lehrstuhl für Netz- und Datensicherheit
Fakultät für Elektrotechnik und Informationstechnik
Horst-Görtz-Institut für IT-Sicherheit
Ruhr-Universität Bochum
Tel.: 0234 32 26798
E-Mail: dennis.felsch@rub.de

Original publication:

Dennis Dennis Felsch, Martin Grothe, Jörg Schwenk, Adam Czubak, Marcin Szymanek: The Dangers of key reuse: practical attacks on IPsec IKE, 2018, Online-Vorabveröffentlichung:
https://www.usenix.org/conference/usenixsecurity18/presentation/felsch

URL for press release: https://www.usenix.org/conference/usenixsecurity18