

Richten Sie die Entschlüsselung auf einem MS Exchange-Server ein

Veröffentlicht: 2025-02-12

Die TLS-Entschlüsselung ist ein leistungsstarkes Tool, um die Sichtbarkeit Ihres Netzwerk zu erhöhen. Die MS Exchange-Sicherheitslücke, CVE-2021-26855, ist ein zwingender Grund, die Entschlüsselung auf Exchange-Servern einzurichten. Diese Schwachstelle ermöglicht es Angreifern, serverseitige Request-Forgery-Angriffe (SSRF) durchzuführen, indem sie maßgeschneiderte HTTP-Anfragen über nicht authentifizierte Verbindungen senden. Diese Anfragen werden normalerweise über HTTPS verschlüsselt. Die einzige Möglichkeit, herauszufinden, ob eine Anfrage diese maßgeschneiderten Anweisungen enthält, besteht darin, die HTTPS-Nutzlasten zu entschlüsseln.

von [Installation einer Sitzungsschlüsselweiterleitung auf Ihrem Exchange-Server](#), können Sie sicherstellen, dass ExtraHop den Exchange-Verkehr sicher entschlüsseln kann. Da CVE-2021-26855 über HTTPS ausgenutzt wurde, empfehlen wir, den HTTP-Verkehr speziell zu entschlüsseln, indem Sie die Anweisungen im folgenden Abschnitt befolgen: [Einen globalen Port zur Protokollzuordnung hinzufügen](#).

Erfahre mehr über [TLS-Entschlüsselung](#).