Sehr geehrte Damen und Herren Kolleginnen und Kollegen,

ich möchte Sie heute über die neusten Entwicklungen hinsichtlich des beA unterrichten.

Wie Sie sicherlich wissen, hat die BRAK die Firma secunet mit der Prüfung der beA-Anwendung beauftragt. Einen Zwischenbericht erstattete secunet den Präsidenten der Regionalkammern am gestrigen Sonntag. Über die Einzelheiten wurde Stillschweigen vereinbart. Secunet bestätigte allerdings, dass nach aktuellem Untersuchungsstand keine Fehler gefunden wurden, die den grundlegenden Aufbau des beA-Systems in Frage stellen. In diesem Zusammenhang darf ich Sie auf die angehängte Pressemitteilung der BRAK vom 15.04.2018 verweisen.

Leider gibt es auch eine weitere unerfreuliche Neuigkeit. Wie die BRAK am 13.04.2018 mitteilte, musste das Bundesweit Amtliche Anwaltsverzeichnis (BRAV) aus Sicherheitsgründen vom Netz genommen werden. Das Online-Magazin Golem.de berichtet hierzu folgendes:

„Wie Golem.de herausgefunden hat, nutzt das offizielle deutsche Rechtsanwaltsregister (Bundesweites Rechtsanwaltsverzeichnis, BRAV) eine veraltete Version der Java-Komponente Primefaces - und die ist für einen Angriff verwundbar, der es aufgrund einer kryptographischen Schwäche erlaubt, Code auf dem Server auszuführen. Damit hätte ein Angreifer theoretisch die Anwaltsdatenbank manipulieren können."

Auch hier darf ich Sie auf die ebenfalls angehängte Pressemitteilung der BRAK verweisen. Den Artikel auf Golem.de finden Sie anliegend.

Soeben hat BRAK-Präsident Schäfer auf der Satzungsversammlung bestätigt, dass laut Atos das BRAV heute - aber spätestens morgen - zur Verfügung stehen wird.

Mit den besten kollegialen Grüßen
Ihr
Herbert P. Schons
Präsident

BUNDESRECHTSANWALTSKAMMER

Presseerklärung Nr. 7 v. 15.04.2018

Secunet berichtet über laufende Prüfung des beA

Auf der heutigen BRAK-Präsidentenkonferenz hat die secunet Security Networks AG den Präsidentinnen und Präsidenten der 28 Rechtsanwaltskammern einen Zwischenbericht zur Sicherheit des besonderen elektronischen Anwaltspostfachs (beA) erstattet.

Die secunet, eine durch das Bundesamt für Sicherheit in der Informationstechnik zertifizierte IT-Sicherheitsdienstleisterin, prüft zurzeit die beA-Anwendung. Die BRAK hatte diese wegen Sicherheitsrisiken im Dezember 2017 vom Netz genommen.

Auftragsgemäß hat secunet eine technische Analyse der beA Client Security und eine konzeptionelle Prüfung der Gesamtlösung des beA inklusive Hardware Security Modul (HSM) vorgenommen.

Secunet bestätigt, dass sie nach aktuellem Untersuchungsstand keine Fehler gefunden haben, die den grundlegenden Aufbau des beA-Systems in Frage stellen. Die bisher festgestellten Schwachstellen des beA-Systems können, so secunet, behoben werden. Die BRAK hat den Entwickler des beA über das vorläufige Zwischenergebnis informiert.

Die Präsidentinnen und Präsidenten waren sich auf ihrer heutigen Sitzung einig, keine inhaltlichen Details zum vorläufigen Zwischenbericht zu veröffentlichen. Die Präsidentenkonferenz folgt damit der ausdrücklichen Empfehlung der Gutachterin, um Risiken z. B. für die IT-Sicherheit der Anwaltschaft auszuschließen, wie sie insbesondere bei nicht erfolgter Deinstallation älterer Versionen der beA-Client Security auf den Rechnern der Nutzer entstehen könnten.

Das umfassende Gutachten der secunet wird nicht vor Mitte Mai vorliegen. Die BRAK wird dann über die weitere Vorgehensweise beraten.

» Startseite » Für Journalisten » Pressemitteilungen - Archiv » 2018 » Presseerklärung 07/2018

BUNDESRECHTSANWALTSKAMMER

Pressemitteilung v. 13.04.2018

Abschaltung des Bundesweiten Amtlichen Anwaltsverzeichnisses (BRAV)

Die Bundesrechtsanwaltskammer hat das Bundesweite Amtliche Anwaltsverzeichnis (BRAV) vorsorglich vom Netz genommen, nach dem eine Sicherheitslücke gemeldet wurde. Weitere Informationen ergeben sich aus anliegenden Rundschreiben des Präsidenten an die Rechtsanwaltskammern. Das BRAV wird nach Behebung der Sicherheitslücke durch den Dienstleister Atos voraussichtlich Anfang nächster Woche wieder online gestellt.

Anlage

» Startseite » Für Journalisten » Pressemitteilungen - Archiv » 2018 » Presseerklärung 06/2018

BUNDESRECHTSANWALTSKAMMER

Der Präsident

Bundesrechtsanwaltskammer
Littenstraße 9 | 10179 Berlin

An alle Rechtsanwaltskammern

BRAK-Nr. 135/2018

Berlin, 13.04.2018

Abschaltung des Bundesweiten Amtlichen Anwaltsverzeichnisses (BRAV)

Sehr geehrte Damen und Herren Kolleginnen und Kollegen,

Herr Böck hat uns über eine Sicherheitslücke im Bundesweiten Amtlichen Anwaltsverzeichnis (BRAV) informiert. Das Online Magazin Golem wird hierüber in Kürze berichten. Diese Sicherheitslücke wurde uns im Verlauf des Vormittags durch die Fa. Atos bestätigt. Zugleich haben wir secunet um eine vorgezogene Prüfung der gemeldeten Komponente gebeten, die erst zu einem späteren Zeitpunkt vorgesehen war. secunet hat die Sicherheitslücke ebenfalls bestätigt.

Wir haben deshalb das BRAV vorsorglich offline gestellt, bis die Fa. Atos den Fehler behoben hat. Dies soll nach Auskunft von Atos Anfang nächster Woche erfolgen, wir rechnen aber nicht vor Dienstag damit. Wir halten Sie informiert.

Mit freundlichen kollegialen Grüßen

Ekkehart Schäfer

Rechtsanwalt Ekkehart Schäfer

Original-URL des Artikels: https://www.golem.de/news/bea-rechtsanwaltsregister-wegen-sicherheitsluecke-abgeschaltet-1804-133825.html **Veröffentlicht:** 13.04.2018 13:51 **Kurz-URL:** https://glm.io/133825

BeA

Rechtsanwaltsregister wegen Sicherheitslücke abgeschaltet

Das deutsche Rechtsanwaltsregister hat eine schwere Sicherheitslücke. Schuld daran ist eine veraltete Java-Komponente, die für einen Padding-Oracle-Angriff verwundbar ist. Das Rechtsanwaltsregister ist Teil des besonderen elektronischen Anwaltspostfachs, war aber anders als dieses weiterhin online.

Die Bundesrechtsanwaltskammer hat ein weiteres Problem mit einer Komponente des besonderen elektronischen Anwaltspostfachs. Wie Golem.de herausgefunden hat, nutzt das offizielle deutsche Rechtsanwaltsregister (Bundesweites Rechtsanwaltsverzeichnis, BRAV) eine veraltete Version der Java-Komponente Primefaces - und die ist für einen Angriff verwundbar, der es aufgrund einer kryptographischen Schwäche erlaubt, Code auf dem Server auszuführen. Damit hätte ein Angreifer theoretisch die Anwaltsdatenbank manipulieren können.

BeA wurde abgeschaltet - das Rechtsanwaltsregister läuft jedoch wieder

Das Rechtsanwaltsregister läuft auf derselben Domain wie das besondere elektronische Anwaltspostfach - kurz BeA. Dieses wurde vor Weihnachten wegen einer Sicherheitslücke abgeschaltet. Doch während das BeA selbst nach wie vor offline ist, wurde das Rechtsanwaltsregister schon nach wenigen Tagen wieder aktiviert.

Zwischenzeitlich hat die Bundesrechtsanwaltskammer die IT-Sicherheitsfirma Secunet beauftragt, die Sicherheit des BeA zu prüfen. Der Anwaltskammer liegt seit kurzem ein erster Zwischenbericht vor. Wie Golem.de erfahren hat, hält die Rechtsanwaltskammer diesen Bericht zur Zeit zurück, da darin Informationen über Sicherheitslücken von noch in Betrieb befindlichen Systemen zu finden seien.

Da das Rechtsanwaltsregister der einzige Teil des BeA ist, der zur Zeit nicht offline ist, war es naheliegend zu vermuten, dass es darin eine weitere Sicherheitslücke geben musste. Golem.de gelang es daher nach kurzer Zeit, diese Lücke zu finden.

Sicherheitslücke in Java-Komponente Primefaces seit 2016 bekannt

Ein Blick in den HTML-Quelltext des Rechtsanwaltsregisters verriet, dass es eine Softwarekomponente namens Primefaces nutzt. In Primefaces wiederum wurde 2016 von der Firma Minded Security eine Sicherheitslücke entdeckt, die es Angreifern erlaubt, auf dem Server Java-Code auszuführen.

Das Problem ist also eine veraltete Java-Komponente. Schon in der BeA-Software selbst war eines der Sicherheitsprobleme, dass zahlreiche veraltete Java-Bibliotheken verwendet wurden. Die Lücke wurde in der im Juni 2016 veröffentlichten Version 6.0 von Primefaces behoben

Zuletzt wurde diese Sicherheitslücke auch laut Berichten im Forum von Primefaces aktiv ausgenutzt und Webseiten damit gehackt. Angreifer hatten damit Cryptocurrency-Miner auf Webseiten installiert.

Rechtsanwaltsregister wurde kurzfristig abgeschaltet

Es gelang uns, diese Sicherheitslücke anhand der Beschreibung von Minded Security im Rechtsanwaltsregister nachzuvollziehen und einen harmlosen Testcode auszuführen. Ein bösartiger Angreifer könnte mit diesem Wissen leicht die Kontrolle über das Rechtsanwaltsregister übernehmen und dort beispielsweise Daten ändern oder auch Malware über die Webseite ausliefern.

Wir haben der Bundesrechtsanwaltskammer empfohlen, aufgrund der Schwere der Lücke das Rechtsanwaltsregister vorläufig abzuschalten. Die Seite ist seit circa 12:40 Uhr am Freitag, den 13. April offline.

Am Sonntag ist ein Treffen der Bundesrechtsanwaltskammer mit den Vorsitzenden der lokalen Rechtsanwaltskammern geplant, dort sollen diese über den Stand der Dinge beim BeA informiert werden.

Verschlüsselte Befehle lassen sich mit Padding Oracle generieren

Die Lücke in Primefaces ermöglicht ein sogenanntes Padding Oracle, eine kryptographische Schwäche, bei der ein Server unterschiedliche Antworten bei der Entschlüsselung einer Blockverschlüsselung gibt und somit dem Angreifer Informationen liefert, die dieser nutzen kann.

Bei Primefaces können verschlüsselte Befehle an ein Interface geschickt werden. Doch die Verschlüsselung hat eine ganze Reihe von Problemen. Zunächst einmal nutzt sie, wenn nicht anders angegeben, ein Standardpasswort. Doch auch wenn man das Passwort ändert, hilft das nichts. Denn die Verschlüsselung nutzt keine Authentifizierung.

Uralte Verschlüsselung, Standardpasswort, fehlende Authentifizierung

Hier kommt das Padding Oracle ins Spiel. Der Server antwortet mit unterschiedlichen HTTP-Codes, je nachdem ob die entschlüsselte Nachricht ein korrektes Padding enthält oder nicht. Damit lassen sich Daten entschlüsseln. Die Grundidee dieses Angriffs hatte 2002 der Kryptograph Sergey Vaudenay erstmals beschrieben.

Zudem nutzt das Ganze eine Verschlüsselung mit dem DES-Algorithmus. Dieser stammt aus den 70ern und lässt sich allein aufgrund der kurzen Schlüssellänge von 56 bit mit einem simplen Brute-Force-Angriff, also dem Ausprobieren aller Schlüssel, knacken. Das ist mit entsprechender Rechenpower in einigen Stunden machbar.

Doch ein Angriff auf DES ist im Fall von Primefaces gar nicht nötig, denn das Padding Oracle bietet einen schnelleren Weg. Damit lassen sich nicht nur Daten entschlüsseln, sondern auch neue Daten verschlüsseln. Mit einigen Hundert Anfragen an den Server kann man somit einen entsprechend verschlüsselten Befehl vorbereiten.

Angriff mit öffentlich verfügbaren Tools durchführbar

Mit einem öffentlich verfügbaren Tool namens Padbuster kann man den Angriff durchführen. Im

Blogpost der Firma Minded Security gibt es dazu eine detaillierte Anleitung.

Der Angriff funktioniert nicht immer, da man den Inhalt des ersten Datenblocks nicht kontrollieren kann. Doch nach einigen Versuchen gelang es uns, einen harmlosen Testcode auszuführen, der einen HTTP-Header einfügt. Da der Server den entsprechenden HTTP-Header in seiner Antwort mit ausgab, konnten wir uns sicher sein, dass die Sicherheitslücke tatsächlich vorhanden und praktisch ausnutzbar ist. (hab)

Verwandte Artikel:
BeA: Secunet findet noch mehr Lücken im Anwaltspostfach
(29.03.2018, https://glm.io/133601)
EGVP: Empfangsbestätigungen einer Klage sind verwertbar
(26.03.2018, https://glm.io/133520)
T-Mobile Österreich: Klartextpasswörter und "amazing Security" bei T-Mobile.at
(07.04.2018, https://glm.io/133713)
OpenSSL-Update: Die Rückkehr des Padding-Orakels
(03.05.2016, https://glm.io/120711)
GNU Patch: Holey Beep verrät Zeroday in Patch-Tool
(06.04.2018, https://glm.io/133703)
