

Pressemitteilung

Einfrieren von Webseiten

Darmstädter Cybersicherheitsforscher decken Schwachstellen
in JavaScript-basierten Webseiten auf

Darmstadt, 05.04.2018. Jeder, der das Internet nutzt, kennt das: Man benötigt dringend Informationen von einer Webseite, möchte eine Buchung durchführen oder einen Online-Einkauf tätigen, doch die gewünschte Webseite startet einfach nicht. Gängige Maßnahmen wie ein Neustart des Rechners oder das Prüfen der WLAN-Verbindung sind nicht immer erfolgreich, manchmal hilft es, einige Zeit abzuwarten und es erneut zu versuchen. Wissenschaftler am Center for Research in Security and Privacy, CRISP zeigen auf, das hinter einem solchen Szenario durchaus auch unlautere Absichten stecken können. Sie haben Schwachstellen in JavaScript Software-Modulen entdeckt, durch die Cyberkriminelle Webseiten gezielt einfrieren können, so dass andere Nutzer nicht mehr auf die Webseite zugreifen können.

Michael Pradel, Professor an der TU Darmstadt und Leiter des Software Labs, überprüft mit seinem Team immer wieder die Webseiten bekannter und auch weniger bekannter Unternehmen und untersucht sie auf Schwachstellen. Dabei konzentriert er sich auf die Webseiten, die JavaScript-basierte Module nutzen.

Bei ihren jüngsten Tests haben Pradel und sein Mitarbeiter Cristian-Alexandru Staicu insgesamt 25 Schwachstellen in JavaScript Software-Modulen aufgedeckt, die immer wieder auf den gleichen Typ zurückzuführen sind. Betroffen sind über 300 Webseiten, deren JavaScript-basierte Server-Implementierung unter sogenannten ReDoS-Schwachstellen leidet. Diese Schwachstellen ermöglichen es, dass eine Webseite durch eine einzige Anfrage regelrecht eingefroren wird. Andere Nutzer können nicht mehr auf diese Seite zugreifen, da der Server, mit dem die Webseite verbunden ist, mit der Bearbeitung dieser einen Anfrage so beschäftigt ist, dass er keine weiteren Anfragen beantworten kann.

Die Wissenschaftler identifizierten hunderte populäre Webseiten, die so durch eine gezielte http-Anfrage für mehrere Sekunden oder sogar Minuten blockiert werden könnten. „Politisch motivierte Angreifer könnten somit eine Webseite gezielt abschalten und damit erreichen, dass unliebsame News zeitverzögert an die Öffentlichkeit gelangen“, erklärt Michael Pradel ein mögliches Szenario. Oder Kunden könnten über eine längere Zeit keine Online-Käufe über die blockierte Webseite durchführen, rufen daraufhin Webseiten der Konkurrenz auf und tätigen dort möglicherweise ihre Einkäufe.

Die Schwachstellen wurden zwischenzeitlich in die Node Security Plattform aufgenommen

- eine Plattform, die Fehlermeldungen in JavaScript-Modulen sammelt und für jeden zugänglich auflistet. Die Anbieter der Module wurden von den Darmstädter Wissenschaftlern ebenfalls informiert und auf die Sicherheitslücken hingewiesen. Erfreulich für Pradel und sein Team – und letztendlich für alle Internet-Nutzer: Die meisten Schwachstellen sind mittlerweile behoben.

Pradel ist mit seinem Team in CRISP, dem europaweit größten Zusammenschluss von Cybersicherheitsforschungseinrichtungen, eingebunden. Dort forscht er an einem der beiden Leuchtturmprojekte des CRISP: den sicheren Web-Anwendungen. Die Wissenschaftler entwickeln skalierbare Programmanalysen für JavaScript-basierte Software, welche Schwachstellen finden und aufdecken sollen. Eine neuartige Kombination von Analysen bei der Ausführung dieser Software und Verfahren zur Generierung von Interaktionssequenzen ermöglicht es, das Verhalten solcher komplexer Internetanwendungen vollautomatisch zu analysieren und Sicherheitslücken aufzudecken.

Über CRISP: Im Center for Research in Security and Privacy (CRISP) haben sich die TU Darmstadt mit ihrem Profilbereich für IT-Sicherheitsforschung CYSEC, die Hochschule Darmstadt sowie das Fraunhofer-Institut für Sichere Informationstechnologie SIT und das Fraunhofer-Institut für Graphische Datenverarbeitung IGD zur europaweit größten Allianz von Forschungseinrichtungen im Bereich Cybersicherheit zusammengeschlossen. Die rund 450 WissenschaftlerInnen beschäftigen sich mit Kernfragen der Cybersicherheit in Gesellschaft, Wirtschaft und Verwaltung. Sie beraten regelmäßig Wirtschaft und öffentliche Verwaltung, geben Hilfestellungen für Firmengründer und erstellen Gutachten für Politik und Wirtschaft.

Bildmaterial: <https://bit.ly/2H9h2ad>

Pressekontakt

Prof. Michael Pradel
TU Darmstadt
Software Lab
Tel.: 06151 16 22390
E-Mail michael.pradel@crisp-da.de

Cornelia Reitz
CRISP
Wissenschaftskommunikation
Tel.: 06151 16 27282
E-Mail: pr@crisp-da.de
www.crisp-da.de