CRISP
Center for Research in Security and Privacy

Press Release

Freezing the Web

Darmstadt's cybersecurity scientists uncover vulnerabilities in JavaScript-based Web Servers

---

Darmstadt, 05.04.2018. Everybody, who uses the Internet, is familiar with the problem: you need information of a web site urgently, want to make a booking or an online-purchase, but the required web site does not load. Common measures, such as restarting your computer or checking the WiFi connection, are not always successful, sometimes it also helps to wait for some time and then try again. Scientists at the Center for Research in Security and Privacy (CRISP) demonstrate that malicious intentions may cause such scenarios. The scientists discovered vulnerabilities in JavaScript software modules, which allow cyber criminals to freeze specific web sites, so that other users cannot access the web site anymore.

Together with his team Michael Pradel, Professor of TU Darmstadt and Head of the Software Lab, checks the web sites of well and lesser known companies and examines them for vulnerabilities. He focuses on web sites that use JavaScript-based modules. During their latest tests Pradel and his employee Cristian-Alexandru Staicu discovered a total of 25 so called ReDoS-vulnerabilities in popular JavaScript software modules. Over 300 web sites, whose JavaScript-based server implementations use these modules are affected. These vulnerabilities allow for a web site to be frozen. Other users are no longer able to access the site, because the server, which is connected to the web site, takes so long for processing one request that it becomes unavailable to all other requests.

The scientists identified hundreds of popular web sites, which can be blocked for some seconds or even minutes by such a well-aimed HTTP request. These vulnerabilities could be used, e.g., by politically motivated attackers to reduce the availability of specific news web sites or by economically motivated attackers to make a competing web site unavailable.

Thanks to the effort of Pradel and Staicu, the vulnerabilities were taken up by the Node Security Platform – a platform, which collects security-related mistakes in JavaScript modules. The module providers were informed by Darmstadt's scientists as well, and were warned about the security breaches. Fortunately for Pradel and his team – and in the end for all Internet users: most of the vulnerabilities have already been removed.

Pradel and his team are part of CRISP, the biggest union of cybersecurity institutes Europe wide. He does research for one of the two flagship projects of CRISP: Secure Web Applications. The scientists develop scalable program analysis for JavaScript-based software, which are to uncover and find vulnerabilities. A new combination of analysis in the execution of this software and methods generating interaction sequences make it possible to analyze the behavior of such complex Web Applications fully automatically and to uncover security breaches.

About CRISP: The Center for Research in Security and Privacy, CRISP, is comprised of the Technische Universität Darmstadt with its CYSEC profile area for IT security research, the Darmstadt University of Applied Sciences, and the Fraunhofer Institute for Secure Information Technology SIT and the Fraunhofer Institute for Computer Graphics Research IGD and is the biggest alliance of research institutes in the area of cybersecurity. About 450 scientists concern themselves with central issues of cybersecurity in society, economy and authorities. They consult the economy and public administration regularly, help company founders and prepare an expert opinion for political and economic use.

Pictures: https://bit.ly/2H9h2ad

Press contact

Prof. Michael Pradel
TU Darmstadt
Software Lab
Tel.: 049 6151 16 22390
E-Mail michael.pradel@crisp-da.de

Cornelia Reitz
CRISP
Science Communication
Tel.: 049 6151 16 27282
E-Mail: pr@crisp-da.de
www.crisp-da.de