idw - Informationsdienst Wissenschaft
Nachrichten, Termine, Experten

Pressemitteilung

CISPA Helmholtz Center for Information Security

Felix Koltermann

26.08.2024
http://idw-online.de/de/news838647

Forschungsergebnisse
Informationstechnik
überregional

Veraltete Codeschnipsel von Stack Overflow gefährden Softwaresicherheit

Eine weit verbreitete Praxis unter Software-Entwickler:innen ist es, sogenannte Codeschnipsel von der Plattform Stack Overflow zu verwenden. Eine Studie des CISPA-Forschers Alfusainey Jallow zeigt jetzt auf, dass damit langfristig Sicherheitsrisiken einhergehen können. Diese liegen unter anderem darin begründet, dass sicherheitsrelevante Updates der Codeschnipsel oft nicht den Weg in die Software finden, in denen sie zum Einsatz kommen. Die Studienergebnisse publizierte Jallow im Paper „Measuring the Effects of Stack Overflow Code Snippet Evolution on Open-Source Software Security" beim IEEE Symposium on Security and Privacy (SP) 2024.

Im Programmier-Alltag stoßen Software-Entwickler:innen immer wieder auf Probleme, für die sie eine schnelle Lösung suchen. „Frühere Studien haben gezeigt, dass die prominenteste Plattform, die Entwickler:innen konsultieren, nicht Lehrbücher sind sondern Stack Overflow", erklärt der CISPA-Forscher Alfusainey Jallow. Stack Overflow gehört zum Netzwerk Stack Exchange und ist eine populäre Onlineplattform für Programmierer:innen und Entwickler:innen, um Antworten auf verschiedene Programmierthemen und -probleme zu finden. „Die Beliebtheit von Stack Overflow liegt daran, dass es funktionale Codeschnipsel anbietet. Ein Codeschnipsel ist eine Verbindung von Code in einer bestimmten Programmiersprache, die ein bestimmtes Problem löst. Man kann ihn meist mit wenigen oder gar keinen Änderungen direkt im eigenen Projekt verwenden", so Jallow weiter.

Suche nach veralteten Codeschnipseln in Github-Projekten

Aus der Forschung ist bereits bekannt, dass es bei den Codeschnipseln auf Stack Overflow auch sicherheitskritische Varianten gibt. Ob der von Stack Overflow kopierte Code sicher ist, lässt sich etwa mit Hilfe von Browser-Plugins überprüfen. Darüber hinaus ist auch bekannt, dass die Codeschnipsel nicht statisch sind, sondern immer weiterentwickelt werden. „Bisher nicht untersucht wurde jedoch die Frage, ob Entwickler, die Codeschnipsel von Stack Overflow in ihre Software kopieren, diese auch updaten, wenn es Veränderungen an den Codeschnipseln auf Stack Overflow gibt", so Jallow. Um dies herauszufinden, haben sich Jallow und seine Kollegen Open-Software-Projekte auf der populären Plattform Github angeschaut. „Github wird verwendet, um Code zu hosten und mit anderen an einem bestimmten Softwareprojekt zusammenzuarbeiten", erklärt der CISPA-Forscher. Zur Durchführung entwickelte er ein mehrstufiges Verfahren, um veraltete Codeschnipsel-Versionen in Github-Projekten zu entdecken und zu überprüfen, ob bei diesen Codeschnipseln sicherheitsrelevante Updates durchgeführt wurden oder nicht.

Fehlende Updates von Codeschnipseln führen zu Sicherheitslücken

In ihrer Untersuchung von knapp 11.500 Github-Projekten kamen Jallow und seine Kollegen zu dem Ergebnis, dass jeder zweite wiederverwendete Codeschnipsel veraltet ist, unabhängig von der verwendeten Programmiersprache. Sie fanden keine Hinweise darauf, dass die GitHub-Entwickler:innen Updates der Codeschnipsel auf Stack Overflow in ihre Projekte übernommen haben. Die mit den Ergebnissen einhergehenden Gefahren liegen laut Jallow in den fast unbegrenzten Verbreitungszirkeln von Software. „Wenn man einen Codeschnipsel aus Stack Overflow kopiert, der die Privatsphäre des Nutzers verletzen kann, und jemand die App auf seinem Handy installiert hat das eine Menge gesellschaftlicher

Auswirkungen. Wenn die Verletzung der Privatsphäre von einem Codeschnipsel von Stack Overflow ausgeht, ist das wirklich ein großes Problem“, ist er überzeugt. Jallow und seine Kollegen ziehen aus ihren Ergebnissen das Fazit, dass „die Entwickler die von Stack Overflow kopierten Snippets nicht auf Änderungen überprüfen, oder sich nicht bewusst sind, dass der von ihnen wiederverwendete Code auf Stack Overflow diskutiert und aktualisiert oder gefixt wird.“

Fehlendes Tool ist ein Auftrag für die Zukunft

Für Entwickler:innen hat Jallow im Moment vor allem eine Empfehlung: „Seid vorsichtig, wenn ihr einen Codeschnipsel von Stack Overflow verwendet. Und wenn ihr welche verwendet, findet einen Weg, um Euch diese zu merken.“ Da es bisher noch kein automatisiertes Tool gibt, bleibt Entwickler:innen nur, selbst immer wieder zu überprüfen, ob es zu den von ihnen verwendeten Codeschnipseln ein Update auf Stack Overflow gibt. Genau das spornt Jallow an, wie er im Gespräch erzählt: „Um diese Lücke zu schließen, würde ich gerne ein Tool entwickeln. Wenn das nicht mehr während meiner Doktorarbeit klappt, dann in einer späteren Karrierephase. Das CISPA hat dieses wirklich tolle Ökosystem, in dem Forschungsergebnisse in die Industrie transportiert werden und Ausgründungen und Startups gefördert werden. Den großen Vorteil, dass es dieses Angebot am CISPA gibt, würde ich gerne nutzen.“

Originalpublikation:

Jallow, Alfusainey and Schilling, Michael and Backes, Michael and Bugiel, Sven
(2024) Measuring the Effects of Stack Overflow Code Snippet Evolution on Open-Source Software Security. In: 45th IEEE Symposium on Security and Privacy.
Conference: SP IEEE Symposium on Security and Privacy

Visualisierung zum Paper „Measuring the Effects of Stack Overflow Code Snippet Evolution on Open-Source Software Security“
CISPA