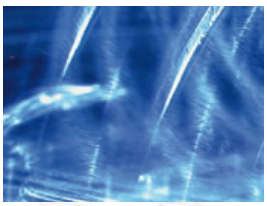

Samsung-Leck bei Sourcecode und Passwörtern - Sicherheitsforscher Mossab Hussein findet grobe Fehler bei Einstellungen des GitLab-Repositorys

Der Sicherheitsexperte Mossab Hussein hat ein gravierendes Sicherheitsleck im System von Samsung entdeckt, wie "TechCrunch" schreibt. Dem Fachmann zufolge bestand das Leak bei zahlreichen Sourcecode-Dateien sowie bei sicherheitsrelevanten Zugangsdaten. Grobe Fehler bei den Einstellungen des GitLab-Repositorys sollen verantwortlich dafür gewesen sein
Das Sicherheitsleck ist deshalb so gravierend, weil eine von Samsung gehostete GitLab-Instanz laut Hussein betroffen waren - ein Ort, wo viele Projekte von Samsung vorangetrieben werden. Möglich war das öffentliche Einsehen für Fachleute wie Hussein nur deshalb, weil ein Mitarbeiter des südkoreanischen Unternehmens offenbar die Projekte als "public" definiert hat. Zusammen mit einem mangelhaften Passwortschutz konnte praktisch jeder die Projekte von aussen einsehen und sich den entsprechenden Sourcecode downloaden.

Konzern spielt Vorfall herunter

Besonders brisant: Nicht nur die Sourcecode-Dateien konnte Hussein finden. Auch stöberte er in einem Projekt die Zugangsdaten zum vollständig genutzten AWS-Zugang auf. Dieser ermöglicht den Zugriff auf 100 sogenannte S3-Storage-Buckets. Diese beinhalten Analysedaten und Log-Dateien, die sich problemlos auslesen lassen konnten. Vor allem umfangreiche Analysedaten zu den SmartThings- und Bixby-Diensten liessen den Sicherheitsforscher aufhorchen. Doch auch private GitLab-Tokens - und das auch noch im Klartext - zu weiteren Projekten waren vorhanden.

So wäre für einen Angreifer der Sourcecode zu manipulieren gewesen, wie Hussein schildert. Eigenen Angaben nach hat er seinen Fund am 10. April Samsung bekannt gegeben. Der Konzern versucht indes die Sache herunterzuspielen und verweist darauf, dass es sich bei der betroffenen Instanz lediglich um eine "Testplattform" gehandelt habe. Das Unternehmen habe zudem bis zum 30. April gebraucht, um die privaten GitLab-Keys zu sperren.