Open Source wider Willen

Massive Sicherheitsprobleme durch offene Git-Repositorys

In Deutschland sind Git-Repositorys auf zehntausenden Servern ungeschützt per Webbrowser zugänglich. Angreifer haben ein leichtes Spiel und können neben Code auch Zugangs- und Nutzerdaten abgreifen.

Von Sylvester Tremmel

Zehntausende von Webservern in Deutschland machen Repositorys des Versionskontrollsystems Git per Browser zugänglich. Die Server veröffentlichen dadurch nicht nur aktuellen und überholten Quellcode, sondern publizieren oft auch Konfigurations- und Zugangsdaten. Zu diesem erschreckenden Befund kommen Sicherheitsexperten der „Deutschen Gesellschaft für Cybersicherheit“ aus Flensburg. Die IT-Fachleute suchten deutsche Internetadressen nach öffentlichen Git-Repositorys ab. Unter 6.927.416 gescannten .de-Domains und -Subdomains fanden sie 41.252 betroffene Systeme, in deren Wurzelverzeichnis ein Repository zugänglich ist.

Die wahre Zahl betroffener Server liegt wahrscheinlich deutlich höher, weil die Flensburger keine Repositorys in Unterverzeichnissen erfassten. Aufgrund der schieren Zahl von Treffern sah sich die Sicherheitsfirma außer Stande, sämtliche Betroffenen zu kontaktieren. Sie wandte sich stattdessen an c’t, die Wochenzeitung Die Zeit und den Norddeutschen Rundfunk, um öffentlich auf die Gefahr hinzuweisen.

In der Tat ist die Liste beeindruckend. Darin finden sich politische Lokalverbände, ebenso wie namhafte IT-Firmen bis hin zu DAX-Konzernen. Betroffen waren beispielsweise Systeme des Versicherungskonzerns Allianz, des Triebwerksherstellers MTU und des Hosting-Anbieters Host Europe. Das Gros sind allerdings private Homepages sowie Webpräsenzen kleinerer Unternehmen. Wie problematisch die Lücke jeweils ist, hängt vom Einzelfall ab. Stichproben ergaben, dass immer wieder auch Konfigurationsdaten in den Archiven sind, die nicht öffentlich bekannt sein sollten. Sogar Zugangsdaten lassen sich oft finden, darunter Passwörter für Datenbankserver. Spätestens in solchen Fällen können Kundendaten bedroht sein. Das ist umso schlimmer, weil sich betroffene Server weitgehend automatisch erfassen und nach Zugangsdaten durchsuchen lassen. Es gibt sogar spezialisierte Browser-Plug-ins, die vor dem Problem warnen und betroffene Repositorys direkt herunterladen.

Kleiner Fehler, große Wirkung

Verantwortlich ist weder eine Sicherheitslücke von Git, noch eine der Webserver-Software. Stattdessen handelt es sich um klassische Fehlkonfigurationen: Git-Repositorys, genauso wie die Archive anderer Versionskontrollsysteme, sollten sich nicht im Web-Root eines Webservers befinden. Wer sie dennoch dort platziert, muss den Webserver entsprechend konfigurieren, um die Archive zu schützen – was die genannten Firmen inzwischen getan haben.

Eigentlich sollte all das hinlänglich bekannt sein. Schon 2015 warnte das Projekt Internetwache.org vor derart fehlkonfigurierten Servern (siehe ct.de/yuqe). Offenbar hat sich deren Warnung bei vielen deutschen Systemadministratoren noch nicht herumgesprochen.

Gegenmaßnahmen

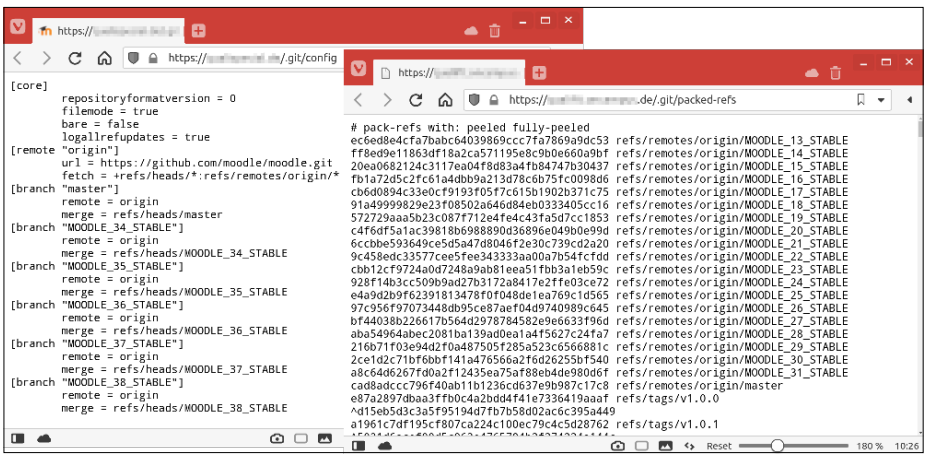
Betroffene sollen den Mangel in jedem Fall schleunigst beheben. Wer sich nicht sicher ist, kann einfach http://meine-domain.de/.git/config im Browser aufrufen. Zeigt der Browser eine Konfigurationsdatei an, ist der Server von dem Problem betroffen. Sie sollten dann entweder das Git-Repository verschieben, sodass es nicht mehr im Web-Root des Servers liegt. Oder Sie konfigurieren den Webserver so, dass Zugriffe auf das Verzeichnis „.git“ unterbunden werden. Ein Artikel der Deutschen Gesellschaft für Cybersicherheit erklärt das Vorgehen für verbreitete Server (siehe ct.de/yuqe).

Directory-Listings zu deaktivieren, ist kein Schutz. Der Webserver liefert dann zwar keine Dateilisten mehr aus, aber gültige URLs lassen sich auch über die interne Struktur von Git-Repositorys konstruieren. Es gibt Tools, die das vollautomatisch erledigen und so ein Repository vollständig herunterladen, ohne auf Dateilisten vom Server angewiesen zu sein.

Die Fälle zeigen, dass Sicherheitsprobleme häufig nicht in technischen Finessen begründet liegen, sondern in Konfigurationsfehlern. Unentschuldbar wird es, wenn die Fehler auch noch seit Jahren bekannt und einfach zu beheben sind.

(syt@ct.de) **ct**

Weiterführende Informationen:
ct.de/yuqe



Git-Repositorys per Browser abrufen zu können ist bestenfalls unnötig und schlimmstenfalls eine gravierende Sicherheitslücke.