

Offene Git-Verzeichnisse gefährden über 40.000 Webseiten deutschlandweit

Flensburg, den 01.07.2020

Die Deutsche Gesellschaft für Cybersicherheit entdeckt mit ihrer Software **cyberscan.io**[®] tausende von Webseiten (23.395 Domains und 41.252 Subdomains), welche von einer bereits bekannten Sicherheitslücke im sogenannten „git-Verzeichnis“ betroffen sind. Insgesamt wurden mit ausgeweiteten Routinescans 6.927.416 Domains und Subdomains aus Deutschland gescannt.

Das Problem ist hierbei eine fehlerhafte Konfiguration des Webservers, welche es Unbefugten ermöglicht, Daten aus dem Verzeichnis herunterzuladen. Oftmals werden sensible Daten (z.B. Quellcodes, Datenbanken, Serverinhalte, Logs, sowie diverse Passwörter und Zugänge) im .git-Verzeichnis hinterlegt und können so extrahiert werden.

Hinweis: Aufgrund der weiten Verbreitung von Git gibt es auch entsprechende Tools, um diese Sicherheitslücke automatisiert aufzuspüren und auszunutzen. Deshalb empfehlen wir diese Lücke schnellstmöglich zu schließen.

Wie können Betroffene herausfinden, ob ihr .git-Verzeichnis öffentlich zugänglich ist?

Der einfachste Weg hierfür ist die Nutzung eines Schwachstellenscanners. Unsere Software **cyberscan.io**[®] zeigt Ihnen die Schwachstelle unter der der Vul-ID 111084 an.

Um manuell herauszufinden, ob eine Domain betroffen ist, müssen Sie zunächst die Domain in die Adresszeile einsetzen und dahinter den Pfad eingeben, um das .git-Verzeichnis aufzurufen (Beispiel: <https://www.Meine-Domain.de/.git/HEAD>).

Folgt auf ihre Anfrage eine Fehlermeldung, so ist der Pfad ins .git-Verzeichnis nicht existent oder abgesichert worden. Erhalten Sie dahingegen eine Meldung, die zum Beispiel „ref: refs/heads/master“ lautet, sind sie von dieser Sicherheitslücke betroffen und sollten den Webserver entsprechend umkonfigurieren.

Hinweis: Wir kontaktieren die Betroffenen mittels einer automatisierten E-Mail, damit sie die Lücke schnellstmöglich schließen können. Unserem Ziel, das Internet jeden Tag etwas sicherer zu gestalten, kommen wir so zusammen ein Stückchen näher.

Wie können Betroffene die Lücke schließen?

Für diese Lücke haben wir für Sie einen Blogbeitrag mit den Lösungswegen für die gängigsten Webserver aufgesetzt. (Link zum [Blog](#)).

Bleiben Sie sicher,
Ihr Team der Deutschen Gesellschaft für Cybersicherheit

Ansprechpartner der Deutschen Gesellschaft für Cybersicherheit:
Ann-Christin Lange; presse@dg-cybersicherheit.de, +49 (0)461 99583873