TRACK und TRACE ausschalten

von Heise-Security

HTTP-Methoden ermöglichen unerlaubtes Ausspähen von Cookies

Ist in einem Cookie die Option httpOnly definiert, darf nur der entsprechende Server darauf zugreifen. Versucht ein Skript den Inhalt des Cookies über die Methode document.cookie abzufragen, wird der Inhalt nicht zurückgeliefert. Damit lassen sich so genannte Cross-Site-Scripting-Attacken (XSS) abwehren. Das CERT/CC weist nun aber in einer Vulnerability Note darauf hin, dass Microsofts Internet Information Server (IIS) eine HTTP-Methode unterstützt, mit der sich solche Cookies trotzdem heimlich ausspähen lassen. Dieses Problem lässt sich allerdings auch analog auf andere Server wie den Apache übertragen.

Zur Fehlersuche ist im HTTP-Protokoll die TRACE-Methode definiert, die als Antwort die ursprüngliche Anfrage eines Web-Clients zurücksendet. Erfordert der Webserver eine Authentifizierung per Cookie, sendet der Client diese mit. In der HTTP-Antwort ist dementsprechend auch das Cookie enthalten. Mit einem Skript kann man nun das Cookie auslesen und anzeigen.

Um nicht das Sicherheitszonen-Modell zu verletzen, darf ein Skript nur mit der Domäne kommunizieren, aus der es stammt. Diverse Fehler in Web-Browsern ermöglichen es aber, Scripting-Code auch in anderen Domänen auszuführen. Damit kann ein Angreifer über eine manipulierte Webseite Code auf einem Client ausführen und über die TRACE-Methode andere Server ansprechen und Cookies auslesen. Diese Art von Angriff bezeichnet man als Cross-Site-Tracing-Angriffe (XST).

Die TRACE-Methode sollte aus Sicherheitsgründen auf Servern im Internet deaktiviert sein, die Anfrage eines Clients bleibt dann ohne Antwort. Ist sie doch aktiviert, schreibt der Server solche Anfragen immerhin in seine Log-Files. Microsoft hat im IIS eine eigene TRACE-Methode implementiert: TRACK. Diese Methode ist zwar nicht vollständig dokumentiert, erfüllt aber weitestgehend den gleichen Zweck wie TRACE. Allerdings loggt der IIS derlei Anfragen nicht mit. Damit kann man einen Angriff nicht mehr nachvollziehen.

Um beim Apache-Webserver die TRACE-Methode zu deaktivieren ist folgende Rewrite-Rule erforderlich:

```
# TRACK und TRACE deaktivieren - http://www.heise.de/security/news/meldung/43354
RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK)
RewriteRule .* - [F,L]
```

Beim IIS lassen sich TRACE- und TRACK-Anfragen mit dem Tool URLScan ausfiltern. Als Methoden sollten nur noch GET, HEAD und POST erlaubt sein.

Revision #1
Created 5 May 2021 07:43:02 by magenbrot
Updated 5 May 2021 07:43:36 by magenbrot